Customer's operational risk towards electronic banking products and its mitigation: a covariance-based structural equation modelling approach

M. Aravind* and Vinith Kumar Nair

TKM Institute of Management,
Musaliar Hills, Karuvelil P.O,
Kollam District, Kerala 691505, India
Email: aravind.1551@gmail.com
Email: vinith79@gmail.com
*Corresponding author

Abstract: The e-banking operations can cause loss or damage to the customers in the form of processing errors, fraud, or via external events. The purpose of this work is to analyse the major risk factors influencing the customers in their e-banking operations. Based on the classic stimulus-response approach, we have identified 15 risk stimuli and four major risk constructs that can cause some encumbrance in e-banking operations. We have also identified some risk mitigation strategies based on the review of literature and focus group discussions. In this work, a stimulus-response model was constructed by linking the operational risk in e-banking with the risk mitigation strategies. Further, we used data from 742 respondents for empirically validating the proposed model. The results of covariance-based structural equation modelling (CB-SEM) revealed that the strategies identified have a positive effect on mitigating the internet banking risk (IBR) only.

Keywords: e-banking; stimulus-response model; risk mitigation; CB-SEM; operational risk.

Reference to this paper should be made as follows: Aravind, M. and Nair, V.K. (2020) 'Customer's operational risk towards electronic banking products and its mitigation: a covariance-based structural equation modelling approach', *Int. J. Electronic Banking*, Vol. 2, No. 1, pp.38–54.

Biographical notes: M. Aravind is an Assistant Professor from the Finance Department at the TKM Institute of Management, Kerala. He has more than a decade of experience in academia and industry. He obtained his MBA and PhD to his credit and also cleared UGC NET in Management. His book entitled, *Principles of Financial Management: Practice and Decisions* was published by Viva Books, New Delhi. He has contributed more than 25 research articles in journals of national and international repute and presented research papers in several seminars and conferences. He is also serving as an external expert in the editorial board of four national journals and one international journal. He is a life member of the Indian Accounting Association.

Vinith Kumar Nair is presently working as a Professor and Associate Dean (External Affairs) at the TKM Institute of Management, Kerala, India. His core areas are innovation, technology interventions, digital marketing, branding, corporate strategy, retailing, sales and managing change. He has more than 18 years of varied experience in industry as well as teaching. He has presented many papers in national and international conferences/seminars and published several research papers in journals of repute. He has authored four books in the field of management and is a business consultant to many organisations.

1 Introduction

The Indian banking system consists of 27 public sector banks and 21 private sector banks. There are 49 foreign banks, 56 regional rural banks, 1,562 urban cooperative banks and 94,384 rural cooperative banks, in addition to cooperative credit institutions. In order to improve the customer service, book-keeping and MIS reporting a need for computerisation was felt in the Indian banking sector in late 1980s. In 1988, the Reserve Bank of India setup a committee on computerisation in banks headed by Dr. C. Rangarajan. Since then banks in India have witnessed a radical change from 'conventional banking to convenience banking'. Today, they are poised for 'digital banking' at a rapid pace. But what is ironical in spite of all these developments is that though the improvement in financial innovations and technologies has made e-banking an intense part of the banking sector India has just 200,000 automatic teller machines (ATMs), 28.8 m credit cards and 818 m debit cards (Reserve Bank of India, 2017).

Banking especially electronic banking involves a variety of risks. From a customer's point of view, the biggest risk that is involved while indulging in electronic banking is the operational risk. This operational risk can arise while using debit cards, credit cards, internet banking (IB) and mobile banking. In this study an attempt has been made to study the customer's operational risk towards electronic banking products. Two focus group discussions were carried out one involving banking customers of different types of banks and one involving the bank employees to identify the operational risk variables and allied mitigation strategies.

We have integrated theoretical models from quantitative perspective as well as from social perspective for defining our research concept. This study has essentially borrowed lessons from the basic stimulus-response models used for risk management (Piegorsch and Bailer, 2005), and the modified version of stakeholder theory suggested by Freeman (1984). Stimulus-response theory is widely used for predicting the quantitative response of some quantitative stimulus as administered by the researcher. In our study various stimulus were quantitatively measured for arriving at the latent constructs viz.; debit card risk (DCR), internet banking risk (IBR), mobile banking risk (MBR), credit card risk (CCR), banker level strategies (BLS), and customer level strategies (CLS). In stakeholder theory it is believed that if a business wants to be successful, it should create value to their customers. Based on the above argument we have modified this theory as the business should try to eliminate all kind of risk arising to its customers on account of their regular interaction.

2 Review of literature

Daniel (1999) defined "e-banking as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels." E-banking service is said to rely on the exchange of information between customers and providers using technological methods devoid of face-to face interaction (Darwish and Lakhtaria, 2011). E-banking may be identified with three channels, namely, ATM, IB and tele banking (Kapoor and Dhingara, 2007).

Earlier studies have demonstrated that the debit card is often a fast and cheap way of paying (Brits and Winder, 2005). A study of three banking technologies in the USA, ATMs, phone banking and IB, found that ATMs had more positive appeal than phone banking, which in turn appealed more than online banking (Curran and Meuter, 2005). But there are studies (Asante-Gyabaah et al., 2015) which show that ATM malfunction, shortage of funds in ATM, ATM card stacking in the machine, etc. are the major drawbacks of ATM Cards. Regarding the usage of debit cards there are studies (Zinman, 2009) which shows that the usage is influenced by relative prices. Studies (Rysman, 2007) have shown that the characteristics of the payment cards industry such as network effects, two sided markets and multi-homing shows that the card usage is highly correlated with the level of acceptance by retailers, too.

From the customers' perspective, IB facilitates a convenient and effective approach to manage personal finances, as it is accessible 24 hours a day and 365 days a year from any locations without the need for visiting the bank (Rotchanakitumnuai and Speece, 2003). Reliability to access the bank's website, high speed of download and upload, high transactions speed of bank's website and short response times from bank's website refer to website features of IB (Jaruwachirathanakul and Fink, 2005). A study has shown that technical terminologies also become the common problems toward end-users to assist them in understanding the security features provided for them (Nowack, 1997). Recent literature on IB also shows that the lacking of trust has to be considered to be one of the main reasons why consumers are still reluctant to conduct their financial transactions online (Flavian et al., 2006; Luarn and Lin, 2005; Mukherjee and Nath, 2003; Rotchanakitumnuai and Speece, 2003). Besides, the usability issues can be looked in term of the performance risk. Performance risk is a situation which occurs due to internal errors of the banking website. For example, server breakdown or internet disconnections may happen which lead to the unpredictable loss (Kuisma et al., 2007). Chauhan and Choudhary (2018) report a negative relationship between attributes such as usage, value, risk, image and tradition barriers with intention to adopt IB. On the other hand guiding and security information was found to have a significant positive relationship with intention to use IB

After realising the importance of simultaneous use of various channels banking and financial companies are now paying attention to mobile banking especially when it comes to maintenance of customer relationships (Riivari, 2005). A study by Wu and Wang (2005) indicated that perceived risk and cost were the variable which significantly affected user behavioural intent. The concepts of risk and trust have emerged together in mobile commerce adoption (Wu and Wang, 2005; Mallat et al., 2008). Sangle and Awasthi (2011) found that the concerns about one's privacy, risk of transaction failure due to low processing speed were among prevalent inhibitors of mobile commerce and mobile internet adoption.

Mitchell and Mickel (1999) define credit cards as source of money which enables the customer to make payments later. The study of Ahmed et al. (2010) found that credit cards across Malaysia might lead to compulsive shopping behaviour causing heavy debt. One of the major risks associated with the use of credit cards is the default risk. In the words of Khare et al. (2012) the financial risks in transaction act as a major deterrent in credit card usage.

The customer's payment choice towards electronic banking options are highly influenced by security and privacy, convenience, and familiarity and ease of use (Hogarth et al., 2008). Customers often think that electronic banking increases chances of government access to public data, increases chances of fraud and data losses (Shabbir et al., 2010). Doubts and hesitation stood as the major concern towards electronic banking usage (Ansari, 2018). To address this issue changes in the mix of manpower deployed in e-lobby branches may have led to improved branch performance (Roy, 2018). A study conducted in Indian context by Kamakodi and Khan (2008) point that there is a wide gap exists in human service in banking while technology-based services are exceeding expectation. To accomplish competitive advantage along with technology the banks have to improve its human services at the branches level. This argument was supported by Alhothaily et al. (2017) as they suggest a user-friendly person-to-person payment system is urgently needed to perform secure and reliable transactions that benefit from current technological advancements.

Security controls are clearly an extremely important issue in e-banking and it is essential for banks to ensure they have established multiple authorisation and authentication measures, identifying the customer wishing to use e-banking services (Abdou et al., 2014). The banks should provide enhanced, new and improved hi-tech security measures such as internet scam protection, hacking detector and anti-virus protections, etc. These upgrades can provide better discretion to both existing and prospective IB customers (Vimala, 2016). Bonneau et al. (2012) through a survey reported that 52.8% of the responders share their ATM/e-transaction PINs with at least one other person. Sharing PIN with others could increase the chance of various payment attacks such as the cloning attack.

3 Objectives and hypotheses

This study was carried out with the aim of assessing the major risk factors influencing the customers in e-banking operations. The major channels in electronic banking are card banking (both debit and credit cards), IB and mobile banking (Singh, 2013). We have identified numerous risk stimuli on the basis of existing theories and literature. Thereafter these risk stimuli were classified under four constructs viz. DCR stimulus, IBR stimulus, MBR stimulus and CCR stimulus. From focus group discussions and from literature some risk mitigation strategies were recognised at banker level (BLS) as well as customer level (CLS). The secondary objective of this research is to fit the most appropriate risk mitigation strategies to relevant risk stimulus for curbing the operational risk in e-banking.

In the light of the theoretical concepts and research objectives the following hypotheses were developed this research.

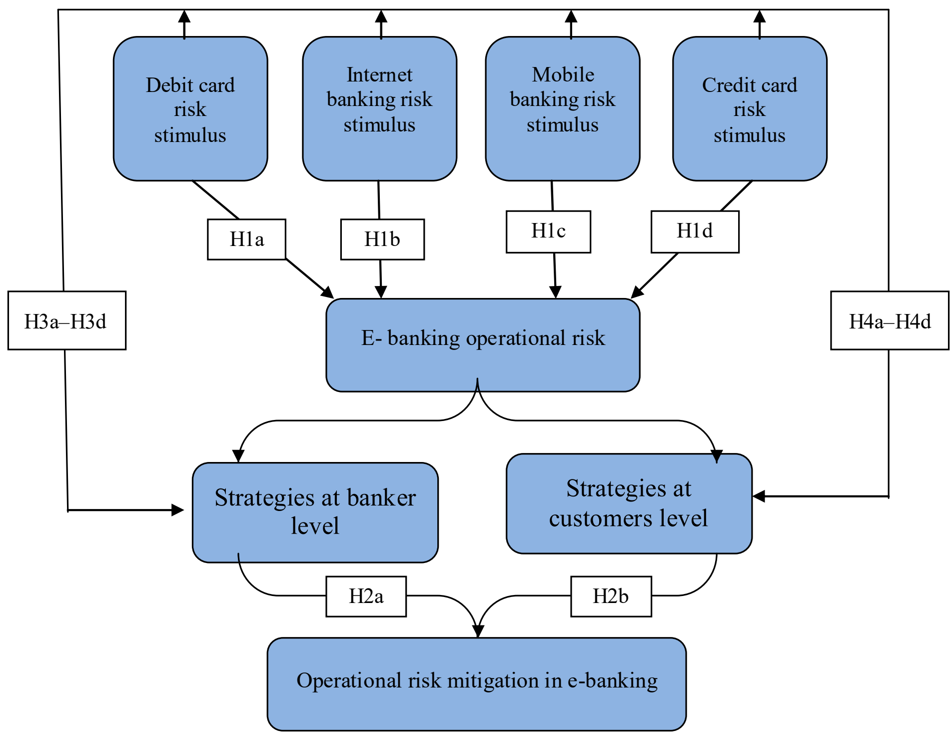
- H1 There is a positive relation between the risk stimulus at customer's level (DCR, IBR, MBR and CCR) and the overall operational risk in e-banking.
- H2 There is a positive relation between risk mitigation stimulus at different levels (BLS and CLS) and operational risk mitigation in e-banking.

H3 There is a positive relation between the strategies formulated at banker level (BLS) and operational risk in e-banking.

H4 There is a positive relation between the strategies formulated at customer level (CLS) and operational risk in e-banking.

Figure 1 exhibits the conceptual framework of this research.

Figure 1 The conceptual model (see online version for colours)



4 Methodology

We have collected the primary data from 742 regular users of e-banking services spread across the Kerala state. The respondent's opinion on operational risk and risk mitigation measures in e-banking was duly collected by employing an exclusively designed questionnaire. The questionnaire for the survey was designed in English and the researchers have used simple random sampling techniques for data collection. Prior to the widespread survey a pilot study has been conducted among 70 respondents from February 2018 to March 2018. The responses obtained from pilot study were scrutinised thoroughly and some open suggestions were incorporated with the instrument. Initially reliability of the responses obtained from pilot study was analysed by using the classical Cronbach's (1951) alpha technique. The factor for which the Cronbach's alpha value is below 0.80 was rechecked and insignificant variables were duly eliminated until getting the critical mark. The significance of items in each factor was determined by computing the inter-item correlation values among variables as recommended by Briggs and Cheek (1986). Based on this criterion we have retained 29 valid statements for the final survey. After obtaining the response from pilot study the final sample size was calculated by using the formula $n \geq (1.96\ \sigma/se)\ 2$. When 'n' is the sample size, 'σ' is the estimate of standard deviation, 'se' is the standard error of the estimate of the population parameter, and the value 1.96 is the critical value from normal test at 5% level of significance. A calculated value of 718 was the maximum among all the responses obtained from different statements. Based on this we have fixed 800 as our sample size. The primary data collection took place over a period of six months from June 2018 to November 2018. During tabulation the unfilled and semi filled questionnaires were eliminated accordingly and finally we have retained 742 valid responses. The characteristics of the sampled data are presented in Table 1.

Table 1 Sample characteristics

Classification	*Description*	*Frequency*	*Percentage*
Age group	Below 25	179	24.10
	26–35	281	37.90
	36–45	156	21.00
	46–60	126	17.00
	Total	*742*	*100.00*
Gender	Male	284	38.30
	Female	458	61.70
	Total	*742*	*100.00*
Education	Secondary	7	0.90
	Higher secondary	152	20.50
	Graduate	345	46.50
	Postgraduate	199	26.80
	Professional degree	39	5.30
	Total	*742*	*100.00*
Occupation	Student	173	23.30
	Govt. employee	112	15.10
	Private/self employed	335	45.10
	Housewives	122	16.40
	Total	*742*	*100.00*
Monthly income	Less than INR 10,000	283	38.10
	INR 10,000–INR 20,000	190	25.60
	INR 20,000–INR 30,000	91	12.30
	INR 30,000–INR 40,000	47	6.30
	Above INR 40,000	131	17.70
	Total	*742*	*100.00*
Source of knowledge about e-banking products	Own accord	224	30.20
	Advertisement in print media	65	8.80
	Online advertisement	20	4.00

Source: Primary data

Table 1 Sample characteristics (continued)

Classification	*Description*	*Frequency*	*Percentage*
Source of knowledge about e-banking products	Referrals groups	177	23.90
	Bank officials	246	33.20
	Total	*742*	*100.00*
The attribute that value most in e-banking service	Service quality	176	23.70
	Technology	216	29.10
	Trust	260	35.00
	Location convenience	90	12.10
	Total	*742*	*100.00*
The most preferred e-banking service	Debit card	282	38.00
	Internet banking	179	24.10
	Mobile banking	158	21.30
	Credit card	123	16.60
	Total	*742*	*100.00*

Source: Primary data

The respondents who participated in the survey were users of different kinds of e-banking services. While observing Table 2 we can realise that this survey was mainly conducted among youth as around 62% of the respondents falling within the age group of below 35. Interestingly among the participants 61.7 percentage were female. The respondents were fairly educated as around 78.6% of them earned a university degree. While considering income 24% of the respondents earning a monthly income over INR 30,000. The major portion of the respondents came to know about e-banking products through own accord and from bank officials with reported frequencies of 30.2% each. The customers' values trust as the most valued attribute in e-banking service as 35% of the respondents enormously marked this variable. The major portions of the respondents were debit card users (38%) and IB occupies the second position with a frequency of 24.1%. Only 16.6% among the respondents preferred to use credit card services clearly signals that the respondents having a conservative attitude towards borrowings.

The model constructs were mostly designed on the basis of variables obtained from literature review. The pilot study conducted among respondents was also stood as a source of identifying key risk variables in e-banking operations. Table 2 shows a complete list of all the individual variables of each factor used in this study.

From Table 2, it can be observed that the constructs DCR and IBR was measured by using five variables each whereas MBR and CCR were measured by using three and two variables respectively. This was on the ground that some statements related to MBR and CCR were eliminated for improving the Cronbach's alpha value. With respect to risk mitigation strategies we have retained seven variables each for the constructs BLS and CLS respectively. In the words of Baumgartner and Homburg (1996), single indicator per construct tends to ignore the unreliability of measurement. Therefore, use of three items is the minimum threshold as a general rule for the number of items per construct. However, in covariance-based (CB)-structural equation modelling this can stand as a major drawback when all factors in the overall model are measured with three items each (Hair et al., 2014). In view of the above argument, we have made a sincere effort to use more than three variables for all major constructs of our model.

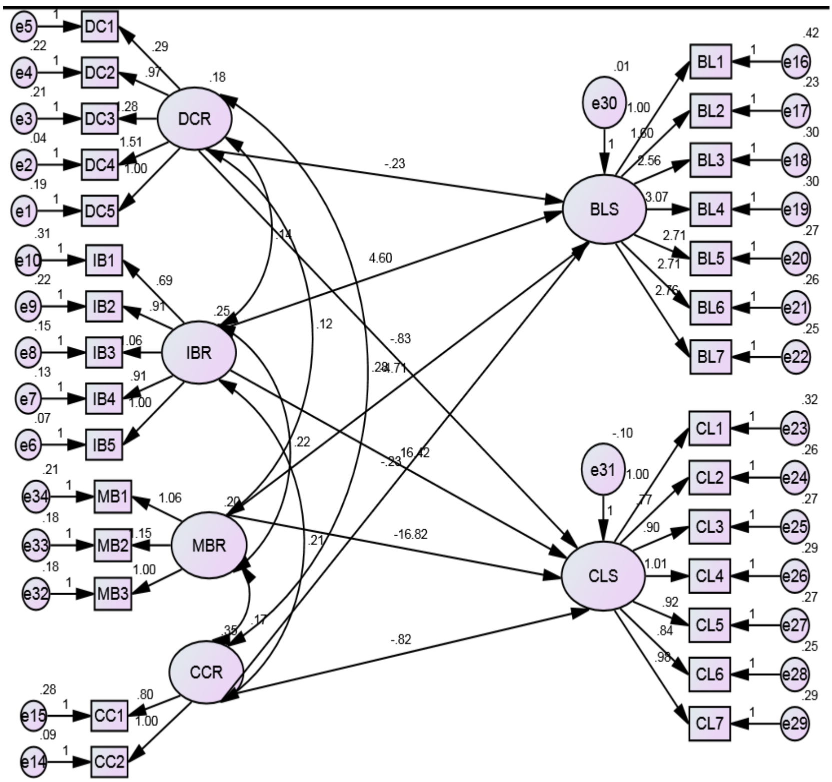
Table 2 Description of study variables

Dimension	*Latent variables*	*No. questions*	*Manifest variables*
Customers operational risk assessment towards e-banking products	Debit card risk (DCR)	5	DC1 → Cards get blocked in ATM machines
			DC2 → Machines out of cash
			DC3 → Non-availability of bank statement
			DC4 → Transaction cost
			DC5 → Level of acceptance for retail transactions
	Internet banking risk (IBR)	5	IB1 → Website navigability
			IB2 → Poor response speed
			IB3 → Security/trust issues
			IB4 → Leaving the operation unfinished
			IB5 → Inconvenience in usage
	Mobile banking risk (MBR)	3	MB1 → Non-availability of mobile applications
			MB2 → Security/trust issues
			MB3 → Low processing speed
	Credit cards risk (CCR)	2	CC1 → Financial risk
			CC2 → Default risk
Customers risk mitigation measures for swift e-banking service	Banker level strategies (BLS)	7	BL1 → User-friendly web portals
			BL2 → Updating e-banking software's
			BL3 → Ensuring sufficient number ATM machines for card transactions
			BL4 → Multiple security measures for online transactions
			BL5 → Web-based digital statement for online/card transactions
			BL6 → Installation of mobile apps by banker
			BL7 → Revising credit limit based on customers risk tolerance level
	Customer level strategies (CLS)	7	CL1 → Use advanced anti-malware program in computers
			CL2 → Deal with reputed web portals/mobile apps
			CL3 → Use only credit cards for online shopping
			CL4 → Do not disclose OTP/PIN number with third parties
			CL5 → Always use a complex password
			CL6 → Pay the credit card dues on time
			CL7 → Check bank account balance at regular intervals

Source: Review of literature and direct interview with respondents

In this research, we have employed covariance-based structural equation modelling (CB-SEM) for processing the data. First of all CB-SEM is a good measure for validating a model with large sample (Tenenhaus, 2008). And it is reported that CB-SEM is useful to examine moderating effect, especially when a third variable changes the relationship between two related variable (Hair et al., 2010). IBM-AMOS.21 version has been used for data analysis. Figure 2 exhibits path diagram of the data used for modelling.

Figure 2 Path analysis (see online version for colours)



5 Data analysis

Initially we have employed reliability test of the independent factors by using the Cronbach's alpha model. The alpha values of the constructs were computed using the estimates of the residuals and its standard error. Sources indicate that an alpha value of 0.8 or above reports sound reliability of the constructs (Cortina, 1993). From Table 3, it can be inferred that the obtained Cronbach's alpha values of the constructs are ranging from 0.942 to 0.869; it is much above the critical level ($\alpha > 0.8$). Likewise composite reliability of the constructs is ranging from 0.890 to 0.764. It is obtained by combining all of the true score variances ($\lambda 2$) of the observed variables related to constructs, and by dividing this sum by the total variance in the constructs. If the composite reliability of the factor loadings are above the threshold 0.7 indicates internal consistency (Hair et al., 2014). The average variance extracted of the factors used in this study is either close or greater than to the generally accepted point of 0.5. If the AVE is 0.5 or more confirms the convergent validity of the factors (Anderson and Gerbing, 1988). We have also checked discriminant validity of the risk assessment constructs in e-banking. It is observed that the square root of the AVE is higher than the correlation between the respective latent variables, confirms discriminant validity (Fornell and Larcker, 1981).

Table 3 Construct reliability and validity

Factors	*Cronbach's alpha*	*Composite reliability*	*Average variance extracted*
DCR	0.942	0.806	0.490
IBR	0.939	0.860	0.559
MBR	0.896	0.784	0.548
CCR	0.869	0.764	0.623
BLS	0.918	0.864	0.490
CLS	0.931	0.890	0.538
Correlation among constructs			

	DCR	*IBR*	*MBR*	*CCR*
DCR	1			
IBR	0.686	1		
MBR	0.615	0.692	1	
CCR	0.563	0.699	0.630	1

Note: Squared correlation among latent variables viz. BLS and CLS has not measured in this model.

Source: Primary data analysis

Table 4 exhibits the result of our CB-SEM model. In this process we have critically examined the effect of observed variables on customer's operational risk towards e-banking as well as the risk mitigation strategies suggested for smooth e-banking practices. As far as operational risk aspect is concerned the observed variables reported to have a strong significant relation with the constructs viz. DCR, IBR, MBR and CCR as the probability value of the test statistics is much below the critical level of 0.05. Additionally, the T-test results are much above the reference point of 1.96. These results strongly signifying Hypotheses 1 (H1a–H1d) by accepting the fact that the observed variables have a significant impact on the constructs. We have also analysed the effect size of each path using f^2 values (Cohen, 1988). In this analysis our f^2 values are ranging from 1.87 to 0.04. A reference point of 0.8 or more indicates large effect between variables. If we are considering the variables individually with respect to DCR the most powerful variable is 'non-availability of bank statement (DC3)' as the reported f^2 value of 1.38 is the highest among other variables. This supports the findings of Asante-Gyabaah et al. (2015) as they have claimed that malfunctioning of ATM's can be a major risk factor in debit card transactions. As far as IBR is concerned the most influential variable is 'security and trust issues (IB3)' with an effect size of 1.87. This result also signifies the findings of early studies carried out by Flavian et al. (2006), Luarn and Lin (2005), Mukherjee and Nath (2003) and Rotchanakitumnuai and Speece (2003). To mitigate this issue customer loyalty along with trust eventually reduces perceived security risk which is vital for further expansion of IB (Mann and Sahni, 2013).

For MBR 'security/trust issues (MB2)' stood as the major risk factor (f^2 = 1.48). Wu and Wang (2005) and Mallat et al. (2008) also reports that the concepts of risk and trust have appeared collectively in mobile banking adoption. Financial risk (CC1) stood as the major risk factor in credit card transactions (f^2 = 1.53). This result confirms the findings of Khare et al. (2012) as they have mentioned that the financial risks in transaction act as a major deterrent in credit card usage.

In our second hypotheses (H2a–H2b) we assumed that the risk mitigation strategies suggested for smooth e-banking operation at various levels are significant. At this stage we have identified seven strategies each from banker's side as well as from customer side. The obtained coefficient (β) for the risk mitigation strategies at this stage are ranging from 3.07 to 0.77. Further the probability values of the test statistics reported to be below the critical line of 0.05 at 95% confidence level. This signifies our null hypotheses. If we are looking at the effect size (f^2 = 1.65) the most preferred risk mitigation strategy at banker level is 'multiple security measures for online transactions (BL 4)'. The customers are on the opinion that 'do not disclose OTP/PIN number with third parties (CL4)' can greatly help to mitigate their risk in e-banking transactions (f^2 = 1.35).

Table 4 CB-SEM result

Path	*Estimates (β)*	*S.E.*	*T-value*	*p-value**	f^2	*Hypotheses*
DC5 → DCR	1.00				0.92	H1a significant
DC4 → DCR	1.51	0.06	25.43	0.00	1.10	
DC3 → DCR	1.28	0.08	17.14	0.00	1.38	
DC2 → DCR	0.98	0.06	17.87	0.00	0.79	
DC1 → DCR	0.29	0.06	5.25	0.00	0.04	
IB5 → IBR	1.00				1.41	H1b significant
IB4 → IBR	0.91	0.03	26.47	0.00	1.56	
IB3 → IBR	1.06	0.04	28.82	0.00	1.87	
IB2 → IBR	0.91	0.04	22.17	0.00	0.92	
IB1 → IBR	0.69	0.05	15.16	0.00	0.38	
MB3 → MBR	1.00				1.07	H1c significant
MB2 → MBR	1.15	0.06	20.27	0.00	1.48	
MB1 → MBR	1.06	0.06	18.87	0.00	1.14	
CC2 → CCR	1.00				1.53	H1d significant
CC1 → CCR	0.80	0.04	20.26	0.00	0.80	
BL1 → BLS	1.00				0.12	H2a significant
BL2 → BLS	1.60	0.19	8.45	0.00	0.57	
BL3 → BLS	2.56	0.29	8.74	0.00	1.15	

Note: *At 5% level of significance.

Source: Primary data analysis

Table 4 CB-SEM result (continued)

Path	*Estimates (β)*	*S.E.*	*T-value*	*p-value**	f^2	*Hypotheses*
BL4 → BLS	3.07	0.35	8.82	0.00	1.65	H2a significant
BL5 → BLS	2.71	0.31	8.84	0.00	1.44	
BL6 → BLS	2.71	0.31	8.83	0.00	1.50	
BL7 → BLS	2.76	0.31	8.85	0.00	1.56	
CL1 → CLS	1.00				1.22	H2b significant
CL2 → CLS	0.77	0.04	18.87	0.00	0.90	
CL3 → CLS	0.90	0.05	19.95	0.00	1.16	
CL4 → CLS	1.01	0.05	20.53	0.00	1.35	
CL5 → CLS	0.92	0.05	20.26	0.00	1.23	
CL6 → CLS	0.84	0.04	19.44	0.00	1.07	
CL7 → CLS	0.98	0.05	20.90	0.00	1.30	
BLS → DCR	–.227	0.17	–1.37	0.17	---	H3a not significant
BLS → IBR	4.60	1.24	3.70	0.00	---	H3b significant
BLS → MBR	–4.71	1.29	–3.65	0.00	---	H3c significant
BLS → CCR	–0.23	0.09	–2.72	0.01	---	H3d significant
CLS → DCR	–0.83	0.61	–1.35	0.18	---	H4a not significant
CLS → IBR	16.42	5.32	3.09	0.00	---	H4b significant
CLS → MBR	–16.82	5.52	–3.05	0.00	---	H4c significant
CLS → CCR	–0.82	0.34	–2.44	0.02	---	H4d significant

Note: *At 5% level of significance.

Source: Primary data analysis

Our third and fourth hypotheses (H3 and H4) examines the cross relationship between the latent constructs used in this study. In the theoretical model we assume that the strategies formulated at banker level (BLS) is sufficient enough to mitigate the customer's operational risk in e-banking (H3a–H3d). Interestingly the results reports that the coefficients obtained at this level for mitigating DCR ($\beta = -2.27$, $t = -1.37$, $p = 0.17$), MBR ($\beta = -4.71$, $t = -3.65$, $p = 0.00$) and CCR ($\beta = -0.23$, $t = -2.72$, $p = 0.01$) is negative. This indicates that the existing strategies identified at the banker level can have a negative influence in mitigating the operational risk of customers. This strongly calls the need for some new and innovative direction to mitigate the customer's operational risk. However, the probability value obtained for DCR do not signifies this negative relation (p-value $0.17 > 0.05$). On the other hand our path analysis clearly produced a positive result for BLS in mitigating operational risk in IB ($\beta = 4.60$, $t = 3.70$, $p = 0.00$). Based on this we can establish a connection among the identified risk factors and strategies. The key risk factor identified for internet banking transaction was security and trust related issues. The same can be easily mitigated through the major strategy identified at the banker level, i.e., use 'multiple security measures for online transactions'. These results support the suggestions of Abdou et al. (2014), and Vimala (2016). In the above studies the authors call for multiple security measures such as hacking detector, anti-virus protection, multiple authentication measures, etc.

We have also formulated some strategies at customer level (CLS) for mitigating e-banking operational risk (H4a–H4d). While testing the hypotheses negative coefficients obtained for the relation with factors DCR (β = –0.83, t = –1.35, p = 0.18), MBR (β = –16.82, t = –3.05, p = 0.00) and CCR (β = –0.82, t = –2.44, p = 0.02) respectively. The coefficient obtained with respect to the CLS → DCR path is not statistically significant at 5% level of significance. Nevertheless the negative coefficients points that the present strategies employed at customers level cannot make any positive influence for extenuating MBR and CCR. With respect to IBR the obtained coefficient is positive and significant (β = 16.42, t = –3.09, p = 0.00). Thereby we can establish a new path for linking the strategies at customer level (CLS) for culminating the IBR. While examining the effect size at IBR level the customers were reported to address the security and trust issues in internet banking transactions. At CLS the most powerful measure identified was ‘do not disclose OTP/PIN number with third parties’. This finding support the study conducted by Bonneau et al. (2012) as this work rightly points that a major portion of the IBR can be mitigated by taking customer centred precaution on secret OTP’s, PIN’s, etc. Taking the above strategies together we can emphasis that the customers should not disclose the OTP/PIN number for online transaction with third parties; and such actions from customer’s level can help in eliminating the risk arising on account of security/trust issues in IB operations.

Table 5 Model fit assessment

Criterion	*Value*	*Norms*	*Inference*
RMSEA	0.018	Value less than 0.08 indicates good fit (MacCallum et al., 1996)	Good fit
NFI	0.891	Value of > .90 indicates fit to the model (Bentler and Bonett, 1980)	Moderate fit
CFI	0.895	Value of > .90 indicates fit to the model (Bentler, 1990)	Moderate fit
PNFI	0.915	Value of > .90 indicates fit to the model (Mulaik et al., 1989)	Good fit

Source: Primary data

Table 5 represents the results of various statistical measures used for assessing the fitness of the established model. The root mean square error approximation (RMSEA) has reported a value of 0.018 and it is much below the threshold limit of 0.08 suggested by MacCallum et al. (1996). The normed fit index (NFI) value of 0.891 and the comparative fit index (CFI) value of 0.895 are much close to the critical mark of 0.90. Parsimonous normed fit index (PNFI) reported with a value of 0.915 is much above the required level of 0.90 (Mulaik et al., 1989). The above measures have confirmed the fitness of the established model.

6 Discussion and policy recommendations

In this work it is observed that all the independent variables found to have a positive and significant relation with the identified factors, this points that the defined items can be a basis in crafting operational risk in e-banking. From risk mitigation angle also the identified strategies found to have a positive and significant relationship with the constructs BLS and CLS. Interestingly it is found that the recognised strategies at both levels are not significant in extenuating DCR. We have observed a negative and significant relationship with the constructs MBR and CCR with the risk alleviation tactics; Whereas IBR is reported to have a positive and significant relationship with the mitigation strategies at both levels. In this connection we can draw an indirect path between IB3 → IBR → BLS → BL4 and IB3 → IBR → CLS → CL4. This can be inferred as the security and trust issues related to IB operations needs to be reduced through implementing multiple security measures at banker level. At the same time the customers have to take some precaution at their level by not disclosing the secret OTP/PIN with third parties. Theoretically this relation can be pinned with the stimulus and response model elaborated by Piegorsch and Bailer (2005). In our model we have drawn a path for representing the relationship between the risk stimulus and the counter responses.

As part of mitigating the operating risks, the banks need to adopt world class technology standards like public key infrastructure (PKI). PKI is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over an increasingly insecure internet. The customers should also be made aware about various security features such as VeriSign, padlock symbol and the letter 's' in the URL. The customers should also be made aware of virtual keyboard feature available on the electronic banking interface page, SMS alerts while a login attempt is made and sign on password expiry. Customers should be sensitised about automatic lockout on multiple incorrect password entry and automatic timeout if account is not operated for a specified period. Customers should be made aware about mandatory use of special characters in password so as to strengthen the password. The banks also need to implement operational risk management practices by recognising operational risk as a separate discipline, restructuring the organisational hierarchy, defining a management process, creating measurement tools and developing monitoring systems (Harris, 2002).

In another context, we have to properly integrate the electronic banking services along with the traditional transactions handled by the human workforce in the branch level. The banks should try to bring a human touch along with the so called electronic banking services. Especially in certain areas such as distribution of passwords to customers, allotment of ATM/credit cards, registration of customers credentials in online portals, etc. Such moves would helps to prevent fraudulent practices to a certain extent. This point supports suggestions from the existing literatures of Kamakodi and Khan (2008), Alhothaily et al. (2017) and Roy (2018).

One of the major limitations of this study is as it elaborates only the path relationship between the constructs and manifest items, and strongly failed to link some strategies for mitigating the operational risk arising on account of debit cards, credit cards and mobile banking. Addition to this we have collected opinion from expert's population only at the time of pilot study through a focus group discussions. However in the later stage of the research we have gathered opinions only from the customers group, this might possibly clogged the opportunity of having more strategies and opinion from the experts group. These limitations could possibly open scope for future research on the topics 'operational risk in card banking and risk alleviation strategies' or 'prudence strategies for card banking through Delphi method'.

References

Abdou, H., English, J. and Adewunmi, P.O. (2014) 'An investigation of risk management practices in electronic banking: the case of the UK banks', *Banks and Bank Systems*, Vol. 9, No. 3, pp.19–31.

Ahmed, Z.U., Ismail, I., Sadiq, S.M., Tabsh, I. and Alias, H. (2010) 'Malaysian consumers' credit card usage behavior', *Asia Pacific Journal of Marketing and Logistics*, Vol. 22, No. 4, pp.528–544.

Alhothaily, A., Alrawais, A., Song, T., Lin, B. and Cheng, X. (2017) 'Quick cash: secure transfer payment system', *Sensors*, Vol. 1376, No. 17, pp.1–20.

Anderson, J.C. and Gerbing, D.W. (1988) 'Structural equation modeling in practice: a review and recommended two-step approach', *Psychological Bulletin*, Vol. 103, No. 3, pp.411–423.

Ansari, Z.A. (2018) 'Barriers to internet banking adoption in developing countries: a consumer survey', *International Journal of Electronic Banking*, Vol. 1, No. 2, pp.171–193.

Asante-Gyabaah, G., Danquah, E. and Tetteh-Wayoe, D. (2015) 'Assessing the impact of the ATM in delivering service in the banking industry. A case of GCB Bank Ltd.', *European Journal of Business and Management*, Vol. 7, No. 20, pp.40–53.

Baumgartner, H. and Homburg, C. (1996) 'Applications of structural equation modeling in marketing and consumer research: a review', *International Journal of Research in Marketing*, Vol. 13, No. 1, pp.139–161.

Bentler, P.M. (1990) 'Comparative fit indexes in structural models', *Psychological Bulletin*, Vol. 107, No. 2, pp.238–246.

Bentler, P.M. and Bonett, D.G. (1980) 'Significance tests and goodness of fit in the analysis of covariance structures', *Psychological Bulletin*, Vol. 88, No. 3, p.588.

Bonneau, J., Preibusch, S. and Anderson, R. (2012) 'A birthday present every eleven wallets? The security of customer-chosen banking PINs', in Keromytis, A.D. (Ed.): *Financial Cryptography and Data Security, FC 2012: Lecture Notes in Computer Science*, Vol. 7397, pp.25–40, Berlin, Heidelberg.

Briggs, S.R. and Cheek, J.M. (1986) 'The role of factor analysis in the development and evaluation of personality scales', *Journal of Personality*, Vol. 54, No. 1, pp.106–148.

Brits, J.H. and Winder, C.C.A. (2005) 'Payments are no free lunch', *DNB Occasional Studies*, Vol. 3, No. 2, De Nederlandsche Bank, Amsterdam.

Chauhan, V. and Choudhary, V. (2018) 'Barriers to adopting internet banking: analysing the influence of information availability and consumer demographics', *International Journal of Financial Services Management*, Vol. 9, No. 3, pp.207–225.

Cohen, J. (1988) *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, NJ.

Cortina, J.M. (1993) 'What is coefficient alpha? An examination of theory and applications', *Journal of Applied Psychology*, Vol. 78, No. 1, p.98.

Cronbach, L.J. (1951) 'Coefficient alpha and the internal structure of tests', *Psychometrika*, Vol. 16, No. 3, pp.297–334.

Curran, J.M. and Meuter, M.L. (2005) 'Self-service technology adoption: comparing three technologies', *Journal of Services Marketing*, Vol. 19, No. 2, pp.103–113.

Daniel, E. (1999) 'Provision of electronic banking in the UK and the republic of Ireland', *The International Journal of Bank Marketing*, Vol. 17, No. 2, pp.72–83.

Darwish, A. and Lakhtaria, K.I. (2011) 'The impact of the new Web 2.0 technologies in communication, development, and revolutions of societies', *Journal of Advances in Information Technology*, Vol. 2, No. 4, pp.204–216.

Flavian, C., Guinaliu, M. and Torres, E. (2006) 'How bricks-and-mortar attributes affect online banking adoption', *International Journal of Bank Marketing*, Vol. 24, No. 6, pp.406–423.

Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, Vol. 18, No. 3, pp.39–50.

Freeman, E.R. (1984) *Strategic Management: A Stakeholder Approach*, Pitman, Boston.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010) *Multivariate Data Analysis*, 7th ed., Prentice Hall, NJ.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014) *A Primer on Partial Least Squares Structural Equation Modeling*, 1st ed., Sage, Thousand Oaks, CA.

Harris, R. (2002) *Emerging Practices in Operational Risk Management*, 24 June, Federal Reserve Bank of Chicago, Chicago, USA.

Hogarth, J.M., Kolodinsky, J. and Gabor, T. (2008) 'Consumer payment choices: paper, plastic, or electrons?', *International Journal of Electronic Banking*, Vol. 1, No. 1, pp.16–35.

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

Kamakodi, N. and Khan, B.A. (2008) 'Looking beyond technology: a study of e-banking channel acceptance by Indian customers', *International Journal of Electronic Banking*, Vol. 1, No. 1, pp.73–94.

Kapoor, S. and Dhingara, D. (2007) 'Application of information technology in banking', in Uppal, R.K. and Rimpi, J. (Eds.): *E-banking in India: Challenges and Opportunities*, New Century Publications, New Delhi.

Khare, A., Khare, A. and Singh, S. (2012) 'Factors affecting credit card use in India', *Asia Pacific Journal of Marketing and Logistics*, Vol. 24, No. 2, pp.236–256.

Kuisma, T., Laukkanen, T. and Hiltunen, M. (2007) 'Mapping the reasons for resistance to internet banking: a means-end approach', *International Journal of Information Management*, Vol. 27, No. 2, pp.75–85.

Luarn, P. and Lin, H-H. (2005) 'Toward an understanding of the behavioral intention to use mobile banking', *Computers in Human Behavior*, Vol. 21, No. 6, pp.873–891.

MacCallum, R.C., Browne, M.W. and Sugawara, H.M. (1996) 'Power analysis and determination of sample size for covariance structure modeling', *Psychological Methods*, Vol. 1, No. 2, pp.130–149.

Mallat, N., Rossi, M., Tuunainen, V.K. and Oorni, A. (2008) 'An empirical investigation of mobile ticketing service adoption in public transportation', *Personal Ubiquitous Computing*, Vol. 12, No. 1, pp.57–65.

Mann, B.S. and Sahni, S.K. (2013) 'Role of trust and customer loyalty in reducing perceived security risk in internet banking', *International Journal of Electronic Business*, Vol. 10, No. 4, pp.331–354.

Mitchell, T.R. and Mickel, A.E. (1999) 'The meaning of money: an individual-difference perspective', *Academy of Management Review*, Vol. 24, No. 3, pp.568–578.

Mukherjee, A. and Nath, P. (2003) 'A model of trust in online relationship banking', *International Journal of Bank Marketing*, Vol. 21, No. 1, pp.5–15.

Mulaik, S.A., James, L.R., Van Alstine, J., Bennet, N., Lind, S. and Stilwell, C.D. (1989) 'Evaluation of goodness-of-fit indices for structural equation models', *Psychological Bulletin*, Vol. 105, No. 3, pp.430–45.

Nowack, M. (1997) 'The impact of the internet on statistical organisations', *Statistical Journal of the UN Economic Commission for Europe*, Vol. 14, No. 4, pp.345–355.

Piegorsch, W. and Bailer, A.J. (2005) *Quantitative Risk Assessment with Stimulus–Response Data. Analyzing Environmental Data*, John Wiley and Sons, West Sussex, England.

Reserve Bank of India (2017) *Bank Wise ATM/POS/Card Statistics* [online] https://rbidocs.rbi.org.in/rdocs/ATM/PDFs/ATMCS08201703C191B257D84D59AE697AB5544DFD67.PDF (accessed 16 October 2017).

Riivari, J. (2005) 'Mobile banking: a powerful new marketing and CRM tool for financial services companies all over Europe', *Journal of Financial Services Marketing*, Vol. 10, No. 1, pp.11–20.

Rotchanakitumnuai, S. and Speece, M. (2003) 'Barriers of internet banking adoption: a qualitative study among corporate customers in Thailand', *International Journal of Bank Marketing*, Vol. 21, Nos. 6–7, pp.312–323.

Roy, A. (2018) 'Business impacts of electronic banking technologies', *International Journal of Electronic Banking*, Vol. 1, No. 2, pp.113–128.

Rysman, M. (2007) 'An empirical analysis of payment card usage', *Journal of Industrial Economics*, Vol. 55, No. 1, pp.1–36.

Sangle, P.S. and Awasthi, P. (2011) 'Consumer's expectations from mobile CRM services: a banking context', *Business Process Management Journal*, Vol. 17, No. 6, pp.898–918.

Shabbir, M.S., Kaleem, A., Kirmani, S. and Qureshi, I.M. (2010) 'Customers' perceptions towards adoption of e-banking in Pakistan', *International Journal of Economics and Business Research*, 2011, Vol. 3, No. 1, pp.1–14.

Singh, T. (2013) *Security and Privacy Issues in E-banking: An Empirical Study of Customers' Perception*, Research Report, October, Indian Institute of Banking and Finance (IIBF), Mumbai.

Tenenhaus, M. (2008) 'Component-based structural equation modeling', *Total Quality Management & Business Excellence*, Vol. 19, Nos. 7–8, pp.871–886.

Vimala, V. (2016) 'An evaluative study on internet banking security among selected Indian bank customers', *Amity Journal of Management Research*, Vol. 1, No. 1, pp.63–79.

Wu, J-H. and Wang, S-C. (2005) 'What drives mobile commerce? An empirical evaluation of the revised technology', *Information & Management*, Vol. 42, No. 5, pp.719–729.

Zinman, J. (2009) 'Debit or credit?', *Journal of Banking & Finance*, Vol. 33, No. 2, pp.358–366.