Asian Journal of Economics and Business. 2(2) **2021 :** pp 127-143

ARF INDIA
Academic Open Access Publishing
www.arfjournals.com

Addressing Information Security in Mobile Banking in the Context of Bangladesh

Md Habibur Rahman[1], Md. Al-Amin[2] and Nusrat Sharmin Lipy[3]

[1]Department of Management Information Systems, Noakhali Science and Technology University, Noakhali-3814, Bangladesh
[2]Department of Management Information Systems, Noakhali Science and Technology University, Noakhali-3814, Bangladesh
[3]Department of Management Studies, University of Barishal, Barishal-8200, Bangladesh
Corresponding author E-mail: habib.nstum@gmail.com

Keywords:

Mobile banking, Risk, Security, Privacy, Security measurement, self-efficacy.

Received: 18 July 2021
Revised: 20 August 2021
Accepted: 22 September 2021
Publication: 30 December 2021

Abstract: With the things go towards information security in mobile banking, measuring and evaluating the status of information security have become one of the key goals for researchers and practitioners. Basically, when it is related to mobile banking view point- whereas considering the security of customers it becomes practically important to address information security of mobile banking. Despite mobile applications being at the frontier of mobile computation technologies, security issues pose a threat to their adoption and diffusion. Recent studies suggest that security violations could be mitigated through improved security behaviors and attitudes, not just through better technologies. Therefore, in this paper some aspects are suggested to maximize information security in mobile banking. Results of multiple regression suggest that Reliable security measure and perceive trust improvement significantly affect self-efficacy and performance (SEP) expectancy of using mobile banking. Results of correlation also support the result of multiple regression. This research highlights the significance of user perceptions of security by examining the content of the security policies of mobile banking for customers' levels. Different security features are discussed that considerably improve upon existing mobile banking systems and allow for seamless integration of our system in the current smart phone context. Appendix A shows different information security improvement issues.

1. Introduction

The evolution of internet services and technologies has affected the operation and management of most commercial and non-commercial systems, including banking services (S.K. Sharma, 2017). While traditional banking services were restricted to bank branches, telephones banking and automated teller machines (ATMs), Mobile Banking has removed such limitations from daily banking activities. As wireless telecommunication and hardware technology are becoming more advanced, the mobile phone/handset is emerging as a powerful computing

and communication platform. The world is moving towards the ever-growing trend of technological adoption. Among other sectors, banking sector is following this emerging trend and has introduced internet banking and mobile banking. Mobile banking refers to the banking activities which can be performed using mobile phones devices (A, Varma, 2018). The mobile technology has become associated with all areas of the industry; it is accelerating and creating new market opportunities for shopping, healthcare service, education and finance etc. The emergence of mobile banking has multiple benefits involving low cost financial services to unbanked population, easier cash handling, investing in assets creation or income generation, reduced vulnerability to cash flow shocks and strong economics by encouraging trade and markets (Y. Yea-Mow Chen, 2000). Bangladesh is one of the growing nationals in the world having 56 commercial banks doing business competitively through the addition of branches, ATMs, POS devices and the internet. But mobile banking is not a mature technology and requires strong face-to-face banking and personal contract. The COVID-19 has made the essence of mobile banking (a way of home banking) inevitable to maintain communication, shopping, banking and many other daily activities.

People normally use mobile devices such as smart phones to access different online services on a daily basis. Many banks are offering mobile banking services which allow bank customers to check balance in their personal account, to transfer funds between accounts and make online payments anywhere and at any time by simply using mobile banking applications installed on their mobile devices (Elkhodr, M., Shahrestani, S., & Kourouche, K, 2012).But, historically trust of the mobile banking technology and perceived security of the transactions play major roles in customers decisions of whether or not to accept internet banking like mobile banking (Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R, 2009). This insecure perception is a major challenge for the adaptation of mobile banking technology and services. The most urgent need of mobile banking users is the enhancement of personal information protection, while offering excellent mobility and convenience, can be easily exposed to various infringement threats. In particular, efforts are required to apply security systems that can preemptively cope with potential threats in the area of banking services, which demand high reliability.

With the development of smart security technologies, the governing rule on security disaster becomes a practical and key issue for mobile financial transactions. Even though mobile banking has become an enormous market,

so far there has been little research on security problems encompassing legal issues in mobile banking (Joyce, 2010). However, as smart phones and mobile banking become more widespread, existing security solutions have become quite fragmented (Horizons, 2008) . People with low income level are major customers of mobile financial services. Now, 15 banks provide mobile financial services having 2.70 crore active client accounts. In February, the average daily transaction through mobile banking was TK.1,425 crore. More than 1.5 million garment workers received salary through Rocket in 1st 10 (ten) day of April 2020 (Shawki, 2020). In an effort to address the increasing threat, researchers and security vendors have been developing new practices, techniques and solutions to reduce security risks associated with mobile banking applications. Mobile banking is a way of financial inclusions of low income customers. So, it requires different supply chain due to product nature (Rahman, 2016). A reliable and secure supply chain dependable to low income people. To help readers understand the state-of-the-art in this fast-moving area, the authors synthesize the related discussions in literature and provide an in-depth review of the security aspect of mobile banking. Currently, the discussion of security risks of mobile banking is disparate, fragmented and distributed in different outlets such as academic articles, white papers, security threat reports and news articles. Mobile malware has been increasing in frequency and has caused a variety of damages including leakage of financial data, financial loss and identity theft (He, W., 2013).

The study focuses on the assessment of information security risks of mobile banking that can influence on the adaptation of mobile banking in Bangladesh. The integrated information security measures for mobile banking services proposed in this paper seems to be utilized effectively when security measures are established for the joint smartphone based mobile banking development project.

2. Literature Review

Mobile banking is an interesting way to go for financial institutions and for customers. Mobile banking has been developed as an effective and convenient channel for financial institutions to distribute their services to clients (Elkhodr M. S., 2012). Behavioral intention towards adoption of mobile banking services was influenced by habit, perceived security, perceived privacy and trust (Mohamed Merhia, 2019). Security remains the biggest concern facing internet banking adoption due to the possibility of data leakage or theft by hackers for example. This has been reflected in many studies, listing security as one of the

most critical barriers facing mobile and e-banking acceptance and growth (B. Sun, 2017). A survey found that when it comes to mobile banking, 31% of customers are willing to pay for added security features, 63% are willing to switch accounts for one with better security features (Heggestuen, 2014).

Among the current growing industry, the mobile communication is growing rapidly and cited as the fastest growing industry in Bangladesh. In the concept of financial presence through mobile banking among the Bangladeshis, has eased the transfer of money through mobile phones, has been getting great attention and interest among the users in the last few years. perceived security protection plays an important role as antecedent of trust. The more the trustee can guarantee the security protection, the trust and intention of customers tend to be higher. Therefore, the trustee must protect the privacy of customers to get trust and continuance intention to mobile banking.

To create a safe and robust mobile banking system, experts have provided different pertinent frameworks and methods for mobile banking security solutions. (Edge, M. E., and Sampaio, P. R. F., 2009) provided a comprehensive survey of existing research into account signatures, an innovative account profiling technology that can improve the fraud detection mechanisms. (Elkhodr M. S., 2012) proposed the Transport Layer Security (TLS) protocol combined with a proposed trust negotiation method, which authenticates the client, the mobile device used in accessing the bank account information, and the server. (J., Ryan W., 2014) as a practitioner from Conference of State Bank Supervisors, suggested a four-step mobile banking risk assessment method, including classification of information, identify threats and vulnerabilities, measure risk and communicate risk. The new plans and solutions on mobile banking cyber security are required in the mobile application development and implementation process. (Sumeet Gupta, 2017) perceived risk and control significantly influenced mobile banking adoption by customers in urban areas, but only perceived control significantly influenced mobile banking adoption by metropolitan customers in India. The New York State Department of Financial Services in 2013 has conducted an industry survey on cyber security and collected information on 154 financial institutions' information security framework and their future plans on cyber security (Cuomo, 2014). Security demotivate users from adopting mobile banking technology. The survey results indicated that increasing sophistication of threats and emerging technologies pose many challenges to security protection. On the other hand, (Pousttchi, 2004) suggested the security requirement for mobile banking: data needs to be encrypted, access to the data

must be authorized and the authorization has to be simple. The study has developed the following hypothesis to conduct the research.

2.1. Risk and Security of Adopting Mobile Banking for Financial Services

Perceived risk refers to the degree of uncertainty in the outcome of using an innovation (Kazemi, 2013). (Pavlou, 2003) defines perceived risk as the user's subjective expectation of suffering a loss in the search for a desired result (Kazi, 2013). The perception of risk is considered an important factor in the use of mobile banking because of the threat to privacy and security concerns (Al-Jabri, 2012). Some studies sustain that the risk perceived by customers is a fundamental obstacle for the future growth of mobile banking services (Luo, 2010). There is a direct relationship between perceived risk and the use of mobile banking.

The security system is a motivation factor for adapting mobile banking by Chinese customers (Luarn, 2005). Security is the most critical issue in customers' intent to adopt mobile banking in Thailand (Speece, 2003). It is an imperative concern and is significant when making e-payments (Tavilla, 2015). Security has become crucial in making mobile banking payment. Commercial banks should invest in a safe, reliable and comprehensive security systems to influence customers in adopting mobile banking.

The customer's perceived risk of the mobile banking service has a negative impact on the use of mobile banking. Perceived risk is considered an element that gives trust its basic nature, which is why customer trust is described according to the perceived risk involved (Kesharwani, 2012). This view makes sense in the context of the use of mobile banking, where there is a physical separation between the bank and the customer, circumstances are difficult to predict, and relationships are difficult to control. Thus, we propose the following hypothesis;

Hypothesis 1: Inherent risk and security (IRS) positively influence self- efficacy and performance (SEP) expectancy of users in adopting mobile banking for financial services.

2.2. Perceived trust (PT) of Adopting Mobile Banking for Financial Services

Trust is the belief of a person to a company in the honesty of its business partner and other factors relevant to this concept (Ganesan, 2003). Perceived trust has been identified as a key barrier to adopt mobile banking for financial services (Gefen, 2003). Trust of the customers need to be formed and very

useful for banks in identifying the barriers of adopting mobile banking for financial services. Primary trust of the user in mobile financial services is the necessary factor for using mobile banking (Koenig-Lewis, 2010).

The generation of trust has been considered a key factor for carrying out online bank transactions. Because there is an absence of any type of practical guarantee, the consumer cannot be sure that the bank will not resort to undesirable opportunistic behaviors (Liébana-Cabanillas, 2016) Some studies show that trust and the perception of risk must be inversely related, such that as the perception of risk increases, the trust in the channel or seller decreases (Liébana-Cabanillas, 2016). Accordingly, the following hypothesis is proposed.

Hypothesis 2: Perceived trust (PT) directly influences self– efficacy and performance (SEP) expectancy of adopting mobile banking for financial services.

2.3. Self-efficacy and Performance Expectancy to Adopt Mobile Banking Services

Mobile banking is expanding in Bangladesh. During the time of Covid-19, the use of mobile banking has been expanded tremendously. Mobile banking is a part of technology. There are different models describing technology acceptance. According to the TAM, attitude construct measures the feeling of favorableness or favorableness towards using the technology (Davis, 1989). However, attitude usually refers to the degree of preference or enjoyment that is derived from the usage of a product or information technology service such as mobile banking (Wang Z. a., 2012).

Self-efficacy in TAM (Viswanath Venkatesh M. G., 2003) is the ability to use technology to accomplish a task. Ease of use is a key factor for consumer acceptance of mobile banking services ((Jeong, 2013). Perceived self-efficacy is a basic capability of using mobile banking (Luarn, 2005). In this research, it is the ability of a user to use mobile banking applications smoothly. It influences more perceived behavioral control to adopt mobile banking than developing an intention. Some studies found direct influence of self-efficacy on mobile banking adoption (Luarn, 2005; Jeong, 2013). Performance expectancy (PE) means incremental job performance of individuals due to mobile banking services (Viswanath Venkatesh J. Y., 2012). PE affects behavioral intention in mobile banking services (Karjaluoto A. A., 2015). Moreover, Mobile payment service adoption is influenced by performance expectancy, perceived security, and mobile payment knowledge (Runhua Peng, 2012). Performance expectancy and self-efficacy come from compatibility, reliability and systems quality influencing adaptation of mobile

banking (Chemingui, 2013). Thus following hypothesis is developed to create reliable and effective mobile banking technologies.

Hypothesis 3: Roeliable security measurement (RSM) can address self-efficacy and performance (SEP) expectancy of adopting mobile banking.

Hypothesis 4: Perceived trust improvement (PTI) can address performance expectancy and self-efficacy of adopting mobile banking.

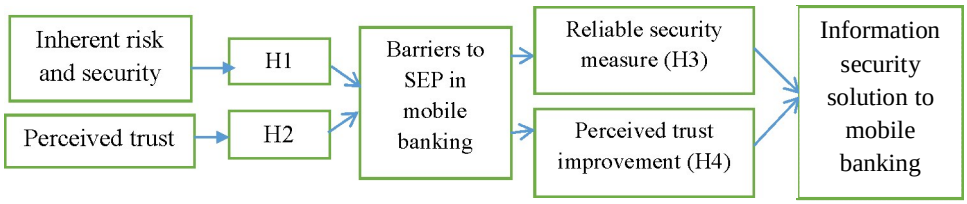

Figure 1: The Proposed Conceptual Framework

Based on the literature review, the study proposes to added reliable security measure and perceived trust improvement to address security problems that may enhance self-efficacy and performance expectancy of adopting mobile banking. Thus in the context of security issues of adopting mobile banking in financial services, the implementation of study results will increase hedonic motivation to use mobile banking reducing risk and increasing trust. The conceptual framework of the study shows the relationship among barriers to self-efficacy and performance expectancy (SEP) in mobile banking with perceived trust (PT) and inherent risk and security (IRS). The study then suggests the possible information security solution for adoption and continuance of mobile financial services. Inherent risk and security of mobile banking and lack of perceive trust demotivate customers to use mobile financial services whereas reliable security measure and perceived trust improvement can address information security and enhance self-efficacy and performance (SEP) expectancy of using mobile financial services. Thus, we propose an extended model to address security issues of mobile banking in figure 1.

3. Methodology

Security in mobile banking, in the context of the present study, includes all individual using or intended to use mobile banking applications through mobile phone in Bangladesh. Hence, the study sample was drawn via convenience sampling from mobile banking application users of Bangladesh. In this study the researcher used quantitative approach of data collection, which was subject

to vigorous quantitative analysis to access the factors influencing consumer's adopting mobile financial services ensuring security. Sample of 303 participants selected randomly consist of both user and non-users of mobile banking. The study mainly uses primary data for analysis purpose.

3.1. Data Collection Procedure and Measurement Scale

An online based questionnaire survey was administrated due to COVID-19 pandemic. The survey was conducted at the users' levels who are using smartphone and have internet connection. The validity of the questionnaires in the study has been assured by assessing questions through various professionals in this field. Before data were collected from final sample, prior analysis was conducted to verify the reliability of the survey that was finally used.

The field was carried out between June and august 2020 through an online self-administrated survey with voluntary participant. The questionnaire recorded on a Likert scale ranging from1 (strongly disagree) to 5 (strongly agree). The second part of the questionnaire was recorded from 1 (very low) to 5 (very high). The last part of the questionnaire indicates innovative measures to be taken to address security issues and enhance performance of using mobile banking for financial services ranging Likert scale from 1 (Very irrelevant) to 5 (Very relevant). Appendix A shows the research questions and measurement scale of the research.

4. Results and Discussion

Table 1: Factor loading*

Measurement items	*Factor 1*	*Factor 2*	*Factor 3*	*Factor 4*	*Factor 5*
IRS1	**.797**	.068	-.082	.130	-.228
IRS2	**.840**	.058	.000	.128	-.027
PT1	.143	-.009	**.703**	-.110	.423
PT3	.055	.102	**.835**	-.011	.032
RSM1	.020	**.749**	-.098	.253	.085
RSM2	.089	**.789**	-.032	.122	.125
RSM3	.024	**.756**	.190	.101	-.086
RSM4	.109	**.780**	-.001	.082	.130
PTI1	-.016	.425	-.062	.169	**.712**
PTI2	.148	.160	.251	-.102	**.724**
PTI3	.019	.134	.747	.145	**.747**
SEP2	.175	-.018	.108	**.790**	.011
SEP3	.046	.065	.186	**.752**	.175

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization

A confirmatory factor analysis with Varimax rotation was conducted to test whether questionnaire items produced the expected number of factors and whether each item was loaded on its appropriate factor in Table 1. All factor loadings below the suggested 0.7 threshold were removed from data analysis (Hair, 2009) . All items show high communality values, indicating that the total amount of variance and original variable shared with all other variables in the analysis is high. Results shown in Table 2 validated that construct measures were valid and, thus, could be used to measure the constructs in the research model.

Table 2: Total variance explained*

Component	*Initial eigenvalues*			*Extraction sums of squared loadings*		
	Total	*% of variance*	*Cumulative %*	*Total*	*% of variance*	*Cumulative %*
IRS1	4.289	26.806	26.806	4.289	26.806	26.806
IRS2	2.346	14.661	41.466			
PT1	1.904	11.900	53.366			
PT3	.890	5.561	65.219			
RSM1	.760	4.751	69.970			
RSM2	.703	4.394	74.364			
RSM3	.450	2.811	91.863			
RSM4	.336	2.103	96.633			
PTI1	.644	4.027	78.391			
PTI2	.612	3.823	82.213			
PTI4	.319	1.996	98.629			
SEP2	.508	3.175	89.053			
SEP3	.219	1.371	100.000			

Extraction Method: Principal Component Analysis

To verify the suitability of data and the measurement scales, exploratory analysis of validity was performed. Validity is the magnitude to which the questions really measure the presence of the variable one aims to measure (Saunders, 2009). The validity of the data in the research study has been assured by assessing questions in the questionnaires for their clarity through various professionals in this field of study.

In order to ensure that the model is free from common method bias, which is a measurement error that threatens the validity of a conclusion drawn upon statistical results (Podsakoff P. M., 2012), the Harman's single factor test, which is most widely used in the literature, (Roni, 2014) was conducted. The result is

obtained by running un-rotated, a single-factor constraint of factor analysis in SPSS. As shown in Table 2, the 26.806% variance explained by a single factor shows that common method bias is not a major concern in this study [less than 50% cut-off point] (Roni, 2014).

Table 3: Correlation matrix and average variance extracted (AVE)

Variables	*Average Variance Extracted (AVE)*	*Square root of AVE*	*IRS*	*PT*	*RSM*	*PTI*	*SEP*
IRS	0.670405	0.802576	1				
PT	0.595717	0.745254	.627**	1			
RSM	0.590865	0.852378	.177**	.167**	1		
PTI	0.52971	0.771569	.120*	.207**	.539**	1	
SEP	0.594802	0.745811	.172**	.182**	.531**	.492**	1

**Correlation is significant at the 0.01 *Correlation is significant at the 0.05

As shown in Table 3, correlation analysis was conducted to test the relationships between variables. The correlation between the Self-efficacy and performance (SEP) of mobile banking and its determinants ranged from 0.172 to 0.531, indicating a high likelihood that these factors influence the attitude toward the usage of mobile banking. The relationship between inherent risk and security (IRS) with Self-efficacy and performance (SEP) expectancy of using mobile banking shows 0.172 (the weakest relationship), between reliable security measure (RSM) with Self-efficacy and performance (SEP) expectancy of using mobile banking shows 0.531 (the strongest relationship), between perceived trust (PT) with Self-efficacy and performance (SEP) expectancy of using mobile banking shows 0.182 (comparatively weak relationship) and between perceived trust improvement (PTI) with Self-efficacy and performance (SEP) expectancy of using mobile banking shows 0.492 (Comparatively strong relationship) to use mobile banking for financial transactions. So, banks should reduce inherent risk and security of adopting mobile banking by implementing reliable security measures first. Security issues have deterred customers from resorting to both e-banking and m-banking options (Bhatt, 2016). Customers willingness to conduct online transaction dependent on perceived privacy control (Zorotheos A. a., 2009). Results show weak relationship between perceived trust and Self-efficacy and performance expectancy of using mobile banking. Therefore, reliable security measurement and perceived trust improvement can lead to address possible information security of adopting mobile banking and improve Self-efficacy and performance expectancy.

The construct validity was also assessed by testing the discriminant validity. Discriminant validity is the extent to which items do not correlate with other items of a different construct (Roni, 2014). In order to test for discriminant validity, the average variance extracted (AVE) for all constructs was calculated to ensure that they are >0.5. The square root of AVE was also compared with the inter-construct correlations. The results in Table 3 demonstrate that the discriminant validity is supported, as the square root of the constructs' AVE is greater than the correlations of the construct with all other constructs (Hulland, 1999; Roni, 2014).

In order to validate the relationship of factors in the research model, a multiple regression analysis was conducted to test the seven (4) hypotheses identified in this study. The dependent variable in this test is the self-efficacy and performance (SEP) expectancy of mobile banking. The independent variables include Inherent risk and security (IRS), Perceived trust (PT), Reliable security measure (RSM) and Perceived trust improvement (PTI). The regression equation was written as follows:

$$SEP_i = \alpha_0 + \alpha_1 IRS_i + \alpha_2 PT_i + \alpha_3 RSM_i + \alpha_4 PTI_i + \varepsilon_i$$

Results from Table 4 show the R2 and Adjusted R2 of 34.7% and 33.8%, respectively, indicating that the factors investigated are suitable to explain attitude toward the usage of mobile banking. The F-stat was reported to be at 52.471 and was significant at a 1% significance level. This also indicates that the combined factors are able to simultaneously explain the SEP quite well.

Table 4: Multiple regression analysis-relationship between factors and security acceptance of mobile banking

Model	*Unstandardized coefficient*		*Standardized coefficients*			*Correlations statistics*			*Collinearity*	
	Beta	*St. error*	*Beta*	*t*	*Sig.*	*Zero-order*	*Partial*	*Part*	*Tolerance*	*VIF*
(Constant)	.716	.238		3.011	.003					
IRS	.036	.038	.057	.947	.344	.172	.055	.044	.599	1.671
PT	.019	.045	.027	.436	.663	.182	.025	.020	.589	1.697
RSM	.454	.070	.364	6.492	.000	.531	.352	.304	.696	1.437
PTI	.302	.060	.283	5.023	.000	.492	.279	.235	.691	1.446
N=303										
R Square	.347									
Adjusted R square	.338									
F-stat	52.471									

Correlation is significant at the 0.01 level.

Regarding each variable factor, results from the multiple regression analysis demonstrated that three out of the two factors were key determinants for whether securities intend to use mobile banking. These factors are reliable security measure (RSM; $\beta = 0.364$) and Perceived trust improvement (PTI; $\beta = 0.283$). In contrast, the results show that the null hypotheses on the relationship between the inherent risk and security (IRS; $\beta = 0.057$) and perceived trust improvement (PTI; $\beta = 0.027$) and self-efficacy and performance (SEP) expectancy of mobile banking cannot be rejected, implying that this factor has negative influence on self-efficacy and performance (SEP) expectancy of mobile banking. The Variance Inflation Factors (VIF) for all factors range between 1.437 and 1.697, which are not greater than 10, indicating that there is no problem of multi-collinearity (Diamantopoulos, 2008).

5. Conclusions of the Study

The main objective of this study was to identify the variables that have the greatest influence on information security in mobile banking in Bangladesh. This is an important issue because it is easy for customers to acquire this type of service, which has enhanced competition and therefore increased the need to build customer loyalty. But certain key barriers for mobile banking adaptation were like security risk and trust. Based on these factors, a model was proposed. This process enabled the identification and integration of the proposed relationships between the variables and made it possible to verify which of these relationships best explains mobile banking users' information security. From the proposed model, the analysis and review of the results shows that the inherent risk and security that have the greatest influence on mobile users' self-efficacy and performance (SEP) expectancy of using mobile banking for financial transactions. Reliable security measures and innovative security measures can enhance the quality and influence loyalty, though indirectly.

The result of the study validates previous studies that perceive security is playing an important role in adopting mobile banking for financial services (Bhatt, 2016). Customers will not perform transactions via a mobile device if they do not trust that such if they trust that their transactions will be kept confidential and secure. Security or privacy threats have significant influence in adopting mobile banking for conducting financial transactions.

Results also show that reliable security measure and perceive trust improvement play a significant role of mobile banking usage. The results in this study validate findings in previous studies, that perceived privacy is a

significant factor in using mobile banking for financial transactions (Liu, 2004). The results show that customers are willing to use mobile banking in the presence of reliable security measures and perceived trust improvement which can be able to maintain the privacy of customer information in mobile banking. Because, they are very much concern to share their information in this site as it related to financial issue. Security, fraud and third party tempering motivates them to develop uncertainty avoidance characteristics like chinses people (Wessels, 2010).

5.1. Implications of the Study

Information security of mobile banking means that banks must systematically and continuously analyze the factors of using mobile banking that lead to user information security (specially privacy of information). The first implication of the study is the development of model that can be used to explain and predict consumers' behavior in terms of protecting their information private. Although, some constructs of the research model studied here have been studied examined in the past, two additional constructs (Reliable security measure and perceive trust improvement) relevant to increase adaptation of mobile banking were identified and examined.

The findings of the present study will help the professionals and mobile banking service providers to develop programs to increase mobile banking adaptation justifying cost and benefits of implementing a mobile banking system, which will address information privacy of users. Banking service providers should focus on managing privacy of information rather than directly influencing intentions to adopt mobile banking.

Our study allows different implications for the companies that make up the green banking management of the users. In our study, both inherent risk and perceive trust, do not achieve a significant effect on self-efficacy and performance (SEP) expectancy of using mobile banking for financial transactions. But, reliable security measure and perceive trust improvement have achieved a significant positive effect on self-efficacy and performance (SEP) expectancy of using mobile banking. Therefore, financial institutions should promote in a sustained manner a type of value added service that will also ensure privacy of customer information.

From a practical standpoint, the findings of the research support reliable security measure (RSM) and perceive trust improvement (PTI) that are significant to enhance self-efficacy and performance (SEP) expectancy of using mobile banking. Financial institutions should ensure such facilities in the mobile banking

technology to adopt or to continue using mobile banking. As, trust is the concern of most people before adopting new technology (Koenig-Lewis, 2010; Gefen, 2003). Customers should also be made aware about the security measure that will ensure privacy of their information.

5.2. Limitations

The study has some limitations as in most empirical studies. The study has considered only two aspects perceive trust (PT) and Inherent risk and security (IRS) to enhance self-efficacy and performance (SEP) expectancy of using mobile banking. But there are some other factors influencing to weaken information security (Koenig-Lewis, 2010; Luarn, 2005). Future research should consider some others security expansion issues and suggest some measurement to enhance self-efficacy and performance (SEP) expectancy of using mobile banking. In addition, a more detail study should be conducted in the future to investigate some features of adopting mobile banking.

Appendix A: Questionnaire and name of measurement scales (ID)

Inherent risk and security (IRS)

Bill payment through mobile banking is a highly insecure way (IRS1)

Account to account fund transfer is insecure. (IRS2)

Perceive trust (PT)

Third party involvement creates possibility to know information by outsiders.(PT1)

Lack of trust in third party agent (pay outlet, cash-out point) motivates me branch banking. (PT2)

I have not much trust to share my personal information in mobile banking web.(PT3)

Reliable security measure (RSM)

Bill payments should be highly secured and safe. (RSM1)

Account to account transfer security should be safe. (RSM2)

Provide Guarantee of payment from user end. (RSM3)

Arrange agreement with internet service provider about trusted service. (RSM4)

Perceive trust improvement (PTI)

Third party tampering should be stopped. (PTI1)

Cash withdrawal at mobile money agents to be risk free. (PTI2)

Provide cash return benefits in incomplete transactions, if user loss money.(PTI3)

Ensure reliable web to give account information. (PTI4)

Self-efficacy and performance (SEP) expectancy

Competency in the technology of mobile banking. (SEP1)

Security enhancement will make a loyal user of mobile banking (SEP2)

Implementation of all measures can motivate me more to mobile banking (SEP3)

References

A, Varma. (2018). Mobile Banking Choices of Entrepreneurs: A Unified Theory of Acceptance and Use of Technology (UTAUT) Perspective. *Theoretical Economics Letters, 8*, 2921.

Al-Jabri, I. &. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research, 13*(4), 379–391.

B. Sun, C. S. (2017). research on initial trust model of mobile banking users. *Journal risk analysis crisis response, 7*(1), 13.

Bhatt, A. (2016). Factors affecting customer's adoption of mobile banking services. *Journal of Internet Banking and Commerce, 21*(1), 1–22.

Chemingui, H. &. (2013). Resistance,motivations, trust and intention to use mobile financial services. *International Journal of Bank Marketing, 31*(7), 574–592. doi:10.1108/IJBM-12-2012-0124

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Diamantopoulos, A. P. (2008). Advancing formative measurement models. *Journal of Business Research, 61*(12), 1203-18.

Edge, M. E., and Sampaio, P. R. F. (2009). A survey of signature based methods for financial fraud detection. *computers & security, 28*(6), 381-394.

Elkhodr, M. S. (2012). A proposal to improve the security of mobile banking applications. *10th International Conference on IEEE* (pp. 260-265). ICT and Knowledge Engineering.

Elkhodr, M. S. (2012). A proposal to improve the security of mobile banking applications. *10th International Conference on IEEE* (pp. 260-265). IEEE.

Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A proposal to improve the security of mobile banking applications. . *10th International Conference on IEEE* (pp. 260-265). ICT & Knowledge Engineering.

Ganesan, S. (2003). Determinant of long-term orientation in buyer–seller relationships. *Journal of Marketing, 2*, 58.

Gefen, D. K. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly, 27*(1), 51–90.

Hair, J. F. (2009). *Multivariate data analysis: A global perspective.* (7th, Ed.) Upper Saddle River: NJ: Prentice Hall.

He, W. (2013). A Survey of Security Risks of Mobile Social Media through Blog Mining and an Extensive Literature Search. *Information Management and Computer Security, 21*(5), 381-400.

Heggestuen, J. (2014). *"The Future Of Mobile And Online Banking*. Retrieved from http://www.businessinsider.com/the-future-of-mobile-and-online-banking-2014-slide-deck.

Horizons, E. (2008). Mobile phones can bring banking within everyone's reach. *Recuperado em*, 20.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*, 195-204.

J., Ryan W. (2014). A Resource Guide for Bank Executives: Executive Leadership of Cybersecurity. *proceedings of the Conference of State Bank Supervisors.*

Jeong, B. K. (2013). An Empirical Investigation on Consumer Acceptance of Mobile Banking Services. *Business and Management Research, 2*(1), 31-40.

Joyce, F. M. (2010). Mobile banking liability: the elephant in the parlor. *Innovator, 3*(3), 29-32.

Karjaluoto, A. A. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics, 32*(1), 129-142.

Kazemi, A. N. (2013). Factors affecting Isfahanian mobile banking adoption based on the decomposed theory of planned behavior. *International Journal of Academic Research in Business and Social Sciences, 3*(7), 230–245.

Kazi, A. K. (2013). Factors affecting adoption of mobile banking in Pakistan: Empirical Evidence. *International Journal of Research in Business and Social Science, 2*(3), 54–61.

Kesharwani, A. &. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing, 30*(4), 303–322.

Koenig-Lewis, N. P. (2010). Predicting young consumers' take up of mobile banking services. *International Journal of Bank Marketing, 28*(5), 410–432.

Liébana-Cabanillas, F. M.-D.-S.-F.-P. (2016). Unobserved heterogeneity and the importance of customer loyalty in mobile banking. *Technology Analysis & Strategic Management*, 1–18.

Liu, C. J. (2004). Beyond concern: A privacy–trust– behavioral intention model of electronic commerce. *Information & Management, 42*(1), 127-142. doi:10.1016/j.im.2004.01.002

Luarn, P. L.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computer in Human Behavior, 21*(6), 873-891. Retrieved from https://doi.org/10.1016/j.chb.2004.03.003

Luo, X. L. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems, 49*(2), 222–234.

Mohamed Merhia, K. H. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, 1-12.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Podsakoff, P. M. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*(1), 539–69.

Pousttchi, K. a. (2004). Assessment of today's mobile banking applications from the view of customer requirements. *Proceedings of the 37th Annual Hawaii International Conference on IEEE.*

Rahman, M. H. (2016). Rahman, M.H., 2016. Impact of Product Nature on Supply Chain in the Global Market: An Analysis of Bangladeshi RMG. *Journal of Business and Economic Development, 1*(1), 14.

Roni, S. M. (2014). *Introduction to SPSS*. Australia: School of Business, Edith Cowan University.

Runhua Peng, L. X. (2012). Exploring Tourist Adoption of Tourism Mobile Payment: An Empirical Analysis. *Journal of Theoretical and Applied Electronic Commerce Research, 7*(1), 21-33.

S.K. Sharma, S. G.-M. (2017). A multi-analytical model for mobile banking adoption: a developing country perspective. *Rev. Int. Business Strategy, 27*(1), 133-148.

Saunders, M. P. (2009). *Saunders, M., Philip, L., & Andrian, T.* Upper Saddle River, NJ: Prentice Hall.

Shawki, S. H. (2020). *Mobile banking services disrupted amid shutdown, clients suffer.* Dhaka: The business standard.

Speece, S. R. (2003). Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand. *International Journal of Bank Marketing, 21*(6/7), 312-323.

Sumeet Gupta, H. Y.-W. (2017). An exploratory study on mobile banking adoption in Indian metropolitan and urban areas: a scenario-based experiment. *Information Technology for Development, 23*(1), 127-152. doi:https://doi.org/10.1080/02681102.2016.1233855

Tavilla, E. (2015). *Transit Mobile Payments: Driving Consumer Experience and Adoption.* Boston: Federal Reserve Bank of Boston.

Viswanath Venkatesh, J. Y. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly, 36*(1), 157-178.

Viswanath Venkatesh, M. G. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Wang, Z. a. (2012). Understanding the intrinsic motivations of user acceptance of hedonic information systems: towards a unified research model. *Communications of the Association for Information Systems, 30*(1), 17.

Wessels, L. D. (2010). An investigation of consumer acceptance of M-banking. *International Journal of Bank Marketing, 28*(7), 547–568.

Y. Yea-Mow Chen. (2000). *The future of banking.* Department of Finance, SanFrancisco State University.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal, 29*(5), 591-65.

Zorotheos, A. a. (2009). Users' perceptions on privacy and their intention to transact online: A study on Greek internet users. *Direct Marketing: An International Journal, 3*(2), 139–53.

To cite this article:

Md Habibur Rahman, Md. Al-Amin and Nusrat Sharmin Lipy (2021). Addressing Information Security in Mobile Banking in the Context of Bangladesh. *Asian Journal of Economics and Business*, Vol. 2, No. 2, pp. 127-143