An Investigation on The Intention to Adopt Mobile Banking on Security Perspective in Bangladesh

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

[1] Department of Management Information Systems, Noakhali Science and Technology University, Noakhali-3814, Bangladesh

[2] Department of Management Studies, University of Barishal, Barishal-8200, Bangladesh

Corresponding: Md. Al-Amin, Assistant Professor, Department of Management Information Systems, Noakhali Science and Technology University, Noakhali 3814, Bangladesh. E-mail: al-amin.mis@nstu.edu.bd

Received: November 14, 2020 Accepted: December 14, 2020 Online Published: December 15, 2020

Abstract

This research examines the information security of adopting mobile banking and suggests maximizing information security in mobile banking in different ways. Security issues pose a threat to mobile banking adoption and diffusion. Therefore, reliable security measures and improved trust improvement are suggested to address information security in adopting mobile banking for financial services. A questionnaire survey is conducted with users of mobile banking technology. Random sampling is adopted in the study. 650 questionnaires were sent to respondents, and 303 responses were recorded. A confirmatory factor analysis with varimax rotation was conducted following correlation and multiple regression analysis to test the hypothesis of the study. The research finds that (1) perceived security and trust affect mobile banking self-efficacy and performance (SEP) of adopting mobile banking for financial services; (2) Reliable security measure and perceive trust improvement positively influence (SEP) of adopting mobile banking for financial services. This study shows the significance of user perceptions of security by inspecting the content of the security rules of mobile banking for clients' levels. It includes the adoption of technology in financial services. Therefore, the study links the technology acceptance model (TAM) with the literature on perceived security and trust of adopting mobile banking for financial services. The research has applied to the banking industry to develop and expand its banking market by developing reliable security measures and improving the perceived trust of customers to conduct banking transactions using mobile banking technology.

Keywords: mobile banking, security, self-efficacy

1. Introduction

The development of internet services and technologies has influenced the activity and the executives of general business and non-business frameworks, including banking services. (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 turning out to be further developed, the mobile phone is becoming a powerful computing and communication tool. The world is going towards the ever-growing trend of technological advancement. Among other sectors, the banking sector is following this trend and has launched internet banking and mobile banking. Mobile banking can be defined as the banking activities which can be done using mobile phone devices (Varma, 2018). Mobile technology has become related to all the fields of the industry; it is quickening 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 the 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 (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 definitely not a full-grown technology and requires strong face-to-face banking and personal agreement. 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 regularly use cell phones, for example, smartphones to access various online services on a day to day basis. Numerous banks are providing mobile banking services that permit bank clients to inquire about the balance in an individual account, to transfer funds between other accounts, and allow online payments anyplace and at any moment by just using mobile banking application platforms installed on their personal phones. (Elkhodr et al, 2012). But, historically trust in the mobile banking technology and perceived security of the exchanges play significant functions in customers' decisions of whether or not to acknowledge web banking like mobile banking (Yousafzai et al, 2009). This insecure perception is a major challenge for the adaptation of mobile banking technology and services. The most urgent need for mobile banking users is the enhancement of personal information protection while offering astounding mobility and convenience, which can be effortlessly presented to different encroachment threats. Specifically, endeavors are needed to apply security structures that can preemptively adjust to expected threats in the field of banking services, which request high dependability.

With the development of smart security technologies, the administering rule on security calamity turns into a big issue for mobile financial transactions. Despite the fact that mobile banking has become a tremendous market, so far there has been little exploration of security issues enveloping lawful issues in mobile banking (Joyce, 2010; Chun, 2007). Nevertheless, as cell phones and mobile banking become more boundless, existing security arrangements have gotten much divided. (Horizons, 2008). People with the lowest income level are significant clients of mobile financial services. Presently, 15 banks offer mobile financial services having 2.70 crore dynamic customer accounts. In February, the normal everyday transactions through mobile banking were TK.1, 425 crores. More than 1.5 million garment workers received salary through Rocket in 1st 10 (ten) days of April 2020 (Shawki, 2020). With an end goal to address the expanding threats, analysts and security merchants have been growing new practices, strategies, and solutions to reduce security risks related to mobile banking applications. Mobile banking is a way of financial inclusion of low-income customers. So, it requires a different supply chain due to its product nature (Rahman, 2016). A reliable and secure supply chain dependable to low-income people. To assist readers with understanding the state-of-the-art in this quick-moving field, the authors blend the related discussions in writing and give an in-depth review of the security aspect of mobile banking. Right now, the conversation of security risks of mobile banking is dissimilar, divided, and appropriated in various sources such as scholarly articles, white papers, security danger reports, and news articles. Mobile malware has been growing in frequency and has been causing a variety of damages including leakage of financial data, financial loss, and identity theft (He, 2013).

The study focuses on the assessment of information security risks of mobile banking that can influence the adaptation of mobile banking in Bangladesh. The organized data safety efforts for mobile financial services proposed in this paper is by all accounts used effectively when safety efforts are set up for the joint wireless-based versatile financial improvement venture.

2. Research Implications

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 (especially privacy of information). The first implication of the research is the development of a research model that can be used to interpret and forecast consumers' behavior in terms of protecting their information private. Albeit a few developments of the exploration model concentrated here have been considered inspected previously, 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 the cost and benefits of implementing a mobile banking system, which will address the information privacy of users. Banking service providers should focus on managing the 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 perceived 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 the privacy of customer information.

From a practical standpoint, the findings of the research support reliable security measures (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 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; Featherman, 2003 & Gefen, 2003). Customers should also be made aware of the security measure that will ensure the privacy of their information.

3. Literature Review and Hypothesis Development

Mobile banking is a fascinating approach for financial institutions and customers. Mobile banking has been made as a powerful and favorable channel for financial institution to circulate their services to clients (Elkhodr et al, 2012). Habit, perceived security, perceived privacy, and trust influence the behavioral intention towards the adoption of mobile banking services (Merhia, 2019). Security remains the greatest concern confronting internet banking adoption because of the chance of data leakage or robbery by programmers for instance. This has been reflected in numerous examinations, posting security as one of the most basic barriers confronting mobile and e-banking acceptance and development (Sun, 2017). Due to the variety of mobile phones and platforms, it is complicated to ensure security on mobile banking (Lee, 2013). A study found that with regards to mobile banking, 31% of customers are eager to pay for added security highlights, 63% are happy to switch accounts for one with better security highlights (Heggestuen, 2014).

Among the current growing industry, mobile communication is developing quickly and referred to as the quickest developing industry in Bangladesh. 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 a vital role as an antecedent of trust. The more the trustee can ensure security protection, the trust and expectation of customers will in general be higher. Therefore, the trustee must protect the privacy of customers to get trust and continuance intention to mobile banking. (Kim, 2008) has proven that perceived privacy protection can influence trust and intention (Zhou, 2014).

To create a protected and vigorous mobile banking framework, specialists have given diverse relevant frameworks and ways for mobile banking security arrangements. (Edge and Sampaio, 2009) gave an exhaustive investigation of a current examination concerning account denotes, an inventive record profiling innovation that can improve the blackmail recognition instruments. (Fatima 2011) prescribes using biometrics to upgrade existing authentication. (Elkhodr et al, 2012) proposed the Transport Layer Security (TLS) protocol joined with a proposed trust exchange strategy, which verifies the customers. In accessing the bank account information and the server, the mobile device is used. According to (Ryan, 2014) as a specialist from the Conference of State Bank Supervisors, recommended a four-step assessment of mobile banking risk strategy, including grouping of information, recognize threats and vulnerabilities, measure risk, and impart risk. The new plans and arrangements on mobile banking cybersecurity are needed in the mobile application improvement and implementation measure. (Gupta, 2017) perceived and control basically influenced mobile banking adoption by clients in metropolitan regions, yet just saw control essentially impacted mobile banking adoption by metropolitan clients in India. The New York State Department of Financial Services in 2013 has directed an industry overview on cybersecurity and gathered data on 154 financial institutions' data security structures and their likely arrangements on cybersecurity (Cuomo, 2014). Security demotivates users from adopting mobile banking technology. The survey results demonstrated that the expanding advancement of threats and arising advances present numerous difficulties to security assurance. Then again, (Pousttchi, 2004) proposed the security necessity for mobile banking: information should be encoded, admittance to the information must be approved and the approval must be straight forward. The study has developed the following hypothesis to conduct the research.

3.1 Risk and Security of Adopting Mobile Banking for Financial Services

Perceived risk can be defined as the degree of uncertainty in the outcome of using an innovation (Kazemi, 2013). (Pavlou, 2003) Portrays perceived risks with regards to the client's emotional desire for enduring a misfortune in the quest for the ideal outcome (Kazi, 2013). The view of risk is considered as a vital factor in the utilization of mobile banking in light of the threat to privacy and security concerns (Ibrahim, 2012). Hardly any investigations proceed with that the danger saw by clients is an essential obstruction for the future development of portable financial administrations (Luo, 2010). There is an immediate connection between perceived risk and the use of mobile banking. The security framework is an inspiration factor for adjusting mobile banking by Chinese customers (Luarn, 2005). Security is the most fundamental issue in clients' arrangements to adopt mobile banking in Thailand (Speece, 2003). It is an imperative concern and is crucial when making e-payments (Tavilla, 2015). Security has become crucial in making mobile banking payments. Commercial banks should invest in safe, reliable, and comprehensive security systems to influence customers in adopting mobile banking.

The customer's perceived risk of mobile banking service negatively affects the utilization of mobile banking. Perceived risk is regarded as a factor that provides trust in its primary nature, which is why customer trust is depicted in order to the perceived risk involved (Kesharwani & Bisht, 2012). This view bodes well with regards to the utilization of portable banking, where there is an actual detachment between the bank and the client, conditions are difficult to envision, and affiliations are very hard 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.

3.2 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 (Featherman, 2003 & Gefen, 2003). Perceived credibility and online banking services have positive significant relation (Wang 2003). Trust of the customers' needs to be formed and very useful for banks in identifying the barriers to adopting mobile banking for financial services. The primary trust of the user in mobile financial services is the necessary factor for using mobile banking (Koenig-Lewis, 2010).

The age of trust has been viewed as a critical factor for performing online banking transactions. Since there is a nonappearance of a useful assurance, the customer can't be certain that the bank won't turn to unfortunate sharp practices (Liébana-Cabanillas, 2016) some studies show that there is an inverse relationship exist in trust and perception of risk, like trust in the channel or seller decreases, the perception of risk increases, (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.

3.3 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. As indicated by the TAM, the attitude build measures the feeling of idealness or idealness towards utilizing the technology (Davis, 1989). Nonetheless, attitude usually refers to the level of preference or enjoyment that is derived from the utilization of a product or information technology service, for example, mobile banking (Wang, 2012).

Self-efficacy in TAM (Venkatesh et al, 2003) is the ability to use technology to accomplish a task. Ease of use can be considered as a vital issue 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 than developing an intention to adopt mobile banking (Yu, 2014). Some studies found a direct influence of self-efficacy on mobile banking adoption (Siddhartha et al, 2011 and Luarn, 2005). Performance expectancy (PE) means incremental job performance of individuals due to mobile banking services (Venkatesh et al, 2012). PE affects behavioral intention in mobile banking services (Karjaluoto, 2015). Moreover, Performance expectancy, perceived security, and mobile payment knowledge influence the adoption of mobile payment systems (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: Reliable 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.

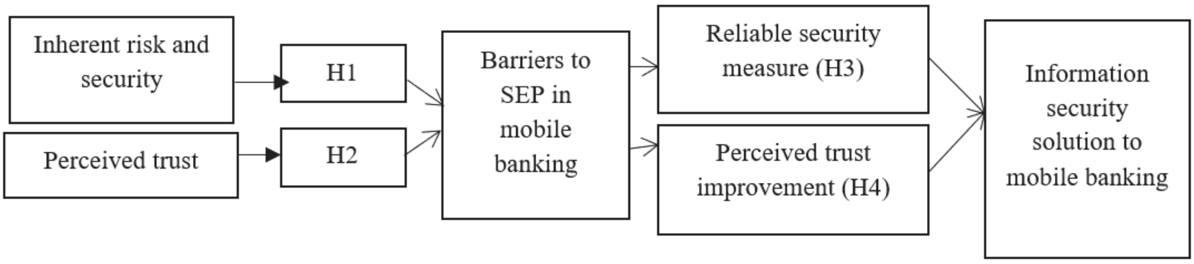
Inherent risk and security
Perceived trust
H1
H2
Barriers to SEP in mobile banking
Reliable security measure (H3)
Perceived trust improvement (H4)
Information security solution to mobile banking

Figure 1. The proposed conceptual framework

Based on the literature review, the study proposes to added reliable security measures 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 the adoption and continuance of mobile financial services. Inherent risk and security of mobile banking and lack of perceived 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 the security issues of mobile banking in figure 1.

4. Methodology

Security in mobile banking, in the context of the present study, includes all individuals using or intended to use mobile banking applications through mobile phones in Bangladesh. Subsequently, the investigation test was drawn by means of comfort examination from mobile banking application clients of Bangladesh. In this study, the researcher used a 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. A sample of 303 participants' response were collected which consist of both user and non-users of mobile banking. The study mainly uses primary data for analysis purposes.

4.1 Data Collection Procedure and Measurement Scale

An online-based questionnaire survey was administrated due to the COVID-19 pandemic. The survey was conducted at the users' levels who are using smartphones and have internet connections. 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 the final sample, the 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 the voluntary participants. 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 the 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 the measurement scale of the research.

4.2 Principal Component Analysis (PCA)

Principal component analysis (PCA) is a way to identify patterns in data and express the data to highlight their similarities and differences. It reduces the number of dimensions without much loss of information. PCA subtracts the mean from each of the data dimensions to produce a data set whose mean is zero (Smith, 2002). It calculates the eigenvectors and eigenvalues for the matrix, while the eigenvector with the highest eigenvalue is the principal component of the data set.

5. Results and Discussion

A confirmatory of the factor examination with varimax pivot was led to test whether the survey things created the normal number of components and whether everything was stacked on its appropriate factor that is presented in Table 1. All the factor loadings in the below-recommended value of 0.7 edges have been taken out from the analysis of data (Hair, 2009) which are also the highest eigenvalue of the data set. Every item expresses high mutuality values, demonstrating that the sum of the variance and unique variable imparted to all other variables the examination is high. Results that appeared in Table 2 confirmed which build measures were valid that could be utilized to measure the developments in the model of the investigation.

Table 1. Factor loading*

Measurement items	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
IRS1	**.797**				
IRS2	**.840**				
PT1		**.703**			
PT3		**.835**			
RSM1			**.749**		
RSM2			**.789**		

RSM3			**.756**		
RSM4			**.780**		
PTI1				**.712**	
PTI2				**.724**	
PTI3				**.747**	
SEP2					**.790**
SEP3					**.752**

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

To verify the suitability of data and the measurement scales, an exploratory analysis of validity was performed. Validity is the greatness to which the questions truly measure the presence of the variable one expects to gauge (Saunders, 2009). Data validity of this research has been guaranteed by examining questions in the survey for the acceptability through different experts in this area of the research.

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 guarantee that the model is liberated from basic strategy inclination, which is an assessment botch that compromises the legitimacy of an end drawn upon factual results (Podsakoff, 2003 & Podsakoff, 2012), the test of the Harman's single factor that is most generally utilized in the writing, (Podsakoff, 2003 & Roni, 2014) was directed. The outcome is gained by running un-rotated, a single factor imperative of figure examination SPSS. As appeared in Table 2, the 26.806% variance clarified by a single factor shows that fundamental technique predisposition is certifiably not a huge concern in this examination [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	0.818782	1				
PT	0.595717	0.771827	.627**	1			
RSM	0.590865	0.768677	.177**	.167**	1		
PTI	0.52971	0.727811	.120*	.207**	.539**	1	
SEP	0.594802	0.771234	.172**	.182**	.531**	.492**	1

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

As presented in Table 3, to test the relationships between variables, a correlation analysis was conducted. The correlation between the performance and Self-efficacy (SEP) of mobile banking and its determinants that ranged from 0.172 to 0.531, demonstrating a high probability that these variables impact the demeanor toward the utilization 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 the inherent risk and security of adopting mobile banking by implementing reliable security measures first. Security issues have discouraged customers from depending on both e-banking and m-banking options (Bhatt 2016). Customers' willingness to conduct online transactions dependent on perceived privacy control (Zorotheos, 2009). Results show a 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 of validity was likewise assessed by testing the discriminant validity. Discriminant validity is how much things don't relate with different things of the alternate construct (Roni, 2014). For the test of discriminant Validity, the average variance extracted (AVE) for all constructs was determined to ensure that they are >0.5. The square foundation of AVE was compared with the inter-construct correlations and they are greater than the average variance extracted. The results in Table 3 exhibit that the discriminant validity is maintained, as the square foundation of the constructs' AVE is more noteworthy than the correlation of the construct with every other construct (Fornell, 1981; Hulland, 1999 and Roni, 2014).

To approve the relationship of factors in the exploration model, a multiple regression analysis was led to test the seven (4) hypotheses recognized in this examination. The dependent variable of 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%, separately, demonstrating that the factors explored are reasonable to clarify demeanor toward the use of mobile banking. The F-stat was accounted for to be at 52.471 and was significant at a 1% significance level. This likewise demonstrates that the consolidated factors can all the while clarify the SEP very well.

Concerning variable factors, results from the multiple regression analysis exhibited 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; β = 0.364) and Perceived trust improvement (PTI; β = 0.283). In the contrast, it is showed that the null hypotheses on the relationship between the inherent risk and security (IRS; β = 0.057) and perceived trust improvement (PTI; β = 0.027) and self-efficacy and performance (SEP) expectancy of mobile banking cannot be rejected, implying that this factor has a negative influence on self-efficacy and performance (SEP) expectancy of mobile banking. The Variance of Inflation Factors (VIF) for all factors which are ranging between 1.437 and 1.697, which are not greater than 10, indicating that there is no problem of multi-collinearity (Diamantopoulos, 2008 & Hair, 2006).

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

Model	Unstandardized coefficient		Standardized coefficients			Correlations			Collinearity statistics	
	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.

6. Conclusions

The main purpose of this study was to identify the variables that have the greatest influence on information security in mobile banking in Bangladesh. This is a significant issue because it is simple 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 security risk and trust. In view of these components, a model was proposed. The highest eigenvalue of principal component analysis used in the hypothesis testing verifies the customers' intention to adopt mobile banking services. Existing mobile banking services involve low perceived trust and inherent risk and security while reliable security measures (RSM) and perceived trust improvement (PTI) can influence users' mobile banking adoption. This cycle empowered the distinguishing proof and incorporation of the proposed connections between the factors and made it conceivable to check which of these connections best clarifies portable financial clients' data security. From the proposed model, the analysis and review of the results show 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 quality and influence loyalty, though indirectly.

The result of this research validates previous studies that perceive security as playing an important role in adopting mobile banking for financial services. 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 a significant influence in adopting mobile banking for conducting financial transactions. Results also show that reliable security measures and perceive trust improvement play a significant role in 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. 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 concerned to share their information on this site as it related to financial issues. Security, fraud, and third-party tempering motivate them to develop uncertainty avoidance characteristics in using mobile banking services for financial transactions.

Mobile banking service providers should consider risk and security issues inherent in mobile banking services seriously and develop mobile banking services for the customers that might lower the inherent risk and security of mobile banking. Reliable security and perceived trust improvement show positive results in adopting mobile financial services.

6.1 Limitations

The study has some limitations as in most empirical studies. The study has considered only two aspects of perceiving 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 and Luarn, 2005). Future research should consider some other security expansion issues and suggest some measurements to enhance self-efficacy and performance (SEP) expectancy of using mobile banking. In addition, a more detailed study should be conducted in the future to investigate some features of adopting mobile banking.

Funding

This research did not receive any external funding.

Conflicts of interest

The authors declare no conflict of interest.

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.

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. https://doi.org/10.1108/IJBM-12-2012-0124

Chun, S. H. (2007). Who is responsible for the onus of proof on online fraud transactions? In perspectives of the eCommerce Law and Privacy Investment. *In Proceedings of The Korea Society of Management Information Systems, Spring 2007* (pp. 699-704). The Korea Society of Management Information Systems.

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

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.

Fatima, A. (2011). E-banking security issues–Is there a solution in biometrics. *Journal of Internet Banking and*

Commerce, 16(2).

Featherman, M. P. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human–Computer Studies, 59*(4), 451-474.

Fornell, C. A. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 1*, 39-50.

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.

H. E. Riquelme, R. R. (2010). the moderating effect of gender in the adoptation of mobile banking. *International journal of bank marketing, 28*(5), 328-341.

Hair, J. F. (2006). *Multivariate data analysis.* Upper Saddle River: NJ: Pearson-Prentice Hall.

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.

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

Ryan W. J. (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.

Kim, D. J. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Decision Support Systems, 44*(2), 544-564.

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

Lee, H. Z. (2013). An Investigation of Features and Security in Mobile Banking. *Journal of International Technology and Information Management, 22*(4).

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.

Lin, H. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledgebased trust. *International journal of information management, 31*(3), 252-260.

Luarn, P. L. H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computer in Human Behavior, 21*(6), 873-891. 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.

Podsakoff, P. M. Y. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 5*, 879–903.

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). 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.

Siddhartha, D., Rik, P., & Sanjay, F. (2011). Factors Affecting Behavioral Intentions towards Mobile Banking Usage: Empirical Evidence from India. *Romanian Journal of Marketing, 6*(1), 6-28.

Smith, L. I. (2002). *A tutorial on Principal Components Analysis.* John Wiley & Sons Inc.

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. 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, Y. S. W. M. H. I. (2003). Determinants of user acceptance of internet banking: an empirical study. *International Journal of Service Industry Management, 14*(5), 501–519.

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.

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.

Yu, C. S. (2014). Consumer switching behavior from online banking to mobile banking. *International journal of cyber society and Education, 7*(1), 1-28.

Zhou, T. A. (2014). Understanding Mobile SNS Continuance Usage in China from The Perspectives of Social Influence and Privacy Concern. *Computers in Human Behavior, 37*, 283-289.

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.

Copyrights