International Journal of Engineering & Technology, 8 (1.4) (2019) 486-491

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Empirical Study of The Indirect Effects of the Perceived Accessibility and Cyber Security of Mobile Banking Applications on User Loyalty to the Applications

Wonjin Jung[1]*,

[1]Dankook University, Korea
**Corresponding author E-mail: jungw@dankook.ac.kr*

Abstract

As the use of smart phones and mobile devices in our daily lives continues to increase today since they were launched in the late 1990s, so do cybercrimes. Because mobile users can use their devices anytime and anywhere and almost without any constraints, mobile devices give users much greater access to the Internet, websites, and mobile applications, and the more users link to networks, the more exposed they are to cyber security issues. Such user mobile network environments have degraded the perceived security of mobile applications. Conventionally, users of mobile banking applications are exposed to potential cybercrimes and sometimes actually experience cyber security incidents. Once users recognize the potential for cybercrimes, they may hesitate or even refuse to use these applications to process their monetary transactions. Under these circumstances, users' perceptions of cyber security issues could limit their loyalty to their mobile banking applications; that is, users could stop using these applications before they even ever form any brand loyalty to the applications. Therefore, it can be inferred that users' loyalty to mobile banking applications is likely to depend on the applications' perceived cyber security. Many information systems (IS) and business researchers have addressed that accessibility and security are critical IS quality attributes. In short, ease of access to mobile banking applications could directly and indirectly affect not only users' perceptions of cyber security and usability but also their loyalty to the applications. But a comprehensive IS and business literature review finds little research on the effects of mobile banking apps' perceived accessibility, security, or usability on user loyalty to the apps. Therefore, The aims of this study are as follows: (1) to examine the direct and indirect effects of the perceived accessibility and cyber security of mobile banking applications on user loyalty to the apps and (2) to find the causal relationships among the perceived accessibility, cyber security, and usability of mobile banking applications and user loyalty to the applications. Structural equation modeling (SEM) was used to analyze the data collected by a survey. The results of analyses show the direct and indirect effects of accessibility of mobile banking apps on the perceived cyber security and usability of the apps as well as on user loyalty to the apps. The results emphasize the importance of perceived accessibility and security in understanding the factors that affect user loyalty to mobile banking applications. The results of this study also indicate that mobile banking applications should provide users with highly accessible but secured systems that make it possible for users to process essential transaction-related information and functions quickly as well as safely.

Keywords: *Accessibiliy: Cyber: Security: Loyalty: Banking Application.*

1. Introduction

As the use of smart phones and mobile devices in our daily lives continues to increase today since they were launched in the late 1990s, so do cybercrimes. Cybercrimes refer to any illegal acts using advanced information technologies, computers, mobile devices, and networks including the Internet. The range of cybercrime is wide from unauthorized access and use, malware and spyware, viruses and hackers, to online theft and fraud [11]. According to some research, millions of cybercrimes take place around the world daily, and these cyber security incidents have tremendous negative effects on the global economy as well as the circumstances of individuals, firms, societies, and countries. Some computer and mobile device activities such as online shopping, banking, and social networking can even put users' safety at risk; whether wired or wireless, as long as users of computer and mobile devices are linked to networks, they need to be aware of cyber security concerns [11].

Because mobile users can use their devices anytime and anywhere and almost without any constraints, mobile devices give users much greater accessibility to the Internet, websites, and mobile applications. Accessibility can be viewed as the "ability to access" and benefit from some system or entity [7]. The concept of accessibility in this study focuses on enabling access for people with special needs, or enabling access through the use of mobile devices . But the more users link to networks, the more exposed they are to cyber security issues [52]. Security mostly refers to the absence of harm or protection from hostile forces [53]. The perception of cyber security in this study is the degree of the absence of harm or the level of protection from any hostile cyber attacks that mobile banking application users perceive when they use their mobile banking apps. Such user mobile network environments have degraded the perceived security of mobile applications [52]. Thus, the following hypothesis is proposed and examined.

Hypothesis 1: The accessibility of mobile banking applications positively affects the perceived cyber security of the applications.

Mobile application users, especially users of mobile banking applications, need to be more careful than PC or ordinary mobile application users.

Conventionally, users of mobile banking applications are exposed to potential cybercrimes and sometimes actually experience cyber security incidents. Once users recognize the potential for cybercrimes, they may hesitate or even refuse to use these applications to process their monetary transactions. Some researchers have stated that the accessibility to and security of mobile applications enable users to communicate safely and quickly with these systems, leading to high perceived usability of the applications [11] Other researchers also have noted that a system's accessibility and security have effects on systems' usability [52].Based on the discussion above, the following hypothesis are proposed and examined.

Hypothesis 2: The perceived cyber security of mobile banking applications positively affects the usability of the applications.

Under these circumstances, users' perceptions of cyber security issues could limit their loyalty to their mobile banking applications; that is, users could stop using these applications before they even ever form any brand loyalty to the applications. Therefore, it can be inferred that users' loyalty to mobile banking applications is likely to depend on the applications' accessibility, usability, and/or perceived cyber security.

Based on the discussion above, the following hypotheses are proposed and examined.

Hypothesis 3: The perceived cyber security of mobile banking applications positively affects the user loyalty to the applications.

Hypothesis 4: The accessibility of mobile banking applications positively affects the perceived usability of the applications.

Hypothesis 5: The perceived usability of mobile banking applications positively affects the user loyalty to the applications.

Hypothesis 6: The accessibility of mobile banking applications positively affects the user loyalty to the applications.

Many information systems (IS) and business researchers have addressed that accessibility and security are critical IS quality attributes. Wang and Strong [18] emphasized the importance of the role of information systems in their data quality framework study and concluded that information systems must be accessible but secure [18]. It can be inferred from their conclusions that the users of mobile banking applications also expect highly accessible but secured applications; when users of these applications realize that the applications are easily accessible but fully secured, then they willingly use the apps to process their financial transactions.

In contrast, when the applications are not easily accessible or secured, users may suspect the usability and usefulness of the applications, which in turn, will have negative effects not only on user intention to use but also on user loyalty to the applications.

In short, ease of access to mobile banking applications could directly and indirectly affect not only users' perceptions of cyber security and usability but also their loyalty to the applications. Thus, the aims of this study are as follows: (1) to examine the direct and indirect effects of the perceived accessibility and cyber security of mobile banking applications on user loyalty to the apps and (2) to find the causal relationships among the perceived accessibility, cyber security, and usability of mobile banking applications and user loyalty to the applications.

2. Methodology

This study explored the impacts that accessibility, perceived cyber security and usability of mobile applications have on the loyalty of the apps. The study achieved this by assessing the levels of accessibility, security, and usability of mobile banking applications that users perceive in the smartphone environment. In this study, these variables were considered mediating variables. A survey was conducted to collect data. Survey is a method or technique aimed at extracting specific data about thoughts, opinions, and feelings from a particular group of people [53].It has been commonly used in the fields of social science for collecting quantitative information about items in a population [5]. Thus, survey is viewed suitable for this study to collect data about the degree of accessibility and security of mobile banking applications that users perceive. Since the smartphone penetration rate is quite high in Korea, the survey was not limited to a certain group of people, but only to the group of people who use mobile banking applications.

This study used Structural equation modeling (SEM), which has been traditionally used to analyze multivariate models [4, 6], so this study employed it to to examine the proposed multivariate research model above. This study also used SPSS Statistics and AMOS ver. 18 as the statistical software for the analysis.

3. Data Analysis and Results

A total of 300 college students and practitioners volunteered to participate in the survey. Two hundred and twenty five students (75% of the participants) answered the questions. The student participants majored in business administration, economics, and computer science at three universities in Korea. The gender ratio of the participants was 60.3% male to 39.7% female (see Table 1). The majority of the participants (77.7%) were in their twenties.

Table 1. Participant Characteristics

	Characteristics	Frequency	Percent
Gender	Males	181	60.3
	Females	119	39.7
	Total	300	100
Age	20-29	233	77.7
	30-39	55	18.3
	40 Above	12	0.4
	Total	300	100

Job	Students	225	75.0
	Practitioners	75	25.0
	Total	300	100

First, the study tested the measurement model by examining the reliability of the individual survey items. The loadings of all items on their respective constructs had to be above 0.6 or ideally 0.7 to comply with the reliability requirements, [6].The results of analysis showed that all of the loadings were of 0.7 or higher, which satisfies the cutoff level of 0.6 (see Table 2). Thus, the results suggest that the reliability is adequate.

Table 2. Standardized Regression Weights of Observable Variables, Composite Reliability (CR), and Average Variance Extracted (AVE)

Latent Variables	**Estimates**	**Variance C.R.**	**Composite Reliability**	AVE
Accessibility	.795	9.512	.933	.746
	.891	7.013		
	.903	6.419		
Perceived security	.844	7.979	.928	.720
	.876	6.919		
	.826	8.455		
Usability	.832	8.728	.955	.749
	.875	7.468		
	.890	6.798		
Loyalty	.867	7.512	.895	.711
	.828	8.717		
	.843	8.235		

This study also examined the convergent and discriminant validity of the measurement model. The composite reliability (CR) and the average variance extracted (AVE) for the constructs were first analyzed to test the convergent validity. With respect to the values of CR and AVE, AMOS ver. 18 does not provide the functions to calculate the values, so they were manually calculated with the formulas, as suggested below by Fornell and Larker [4] and Hair et al. [6]. The results of the analyses showed that the CR values of all constructs were greater than the recommended level of 0.7 (see Table 4). In addition, the results also showed that the values for the AVE of all constructs in the model were 0.7 or higher, which is well above the recommended level of 0.5 (see Table 4). Therefore, the measurement model demonstrated a satisfactory convergent validity.

$CR = (\sum \text{Standard Regr. Weights})^2 /$ er (1981)
$((\sum \text{Standard Regr. Weights})^2 + (\sum \text{Var.}))$. [4]
al. (2006)
$AVE = (\sum \text{Standard. Regr. Weights}^2) /$
N. [6]

On the other hand, the discriminant validity for the measurement model was tested by comparing the square root of the AVE with the correlations among the constructs. The results of analyses for the discriminate validity showed that each construct had a square root of the AVE greater than the correlations between the construct and the other constructs (see Table 3). This indicates that the measurement model of this study satisfies the requirements of the discriminant validity.

Table 3. Correlation Coefficient Value between Constructs and AVE

Constructs	**AVE**	$ø^2$	$ø^2$	$ø^2$	$ø^2$	$ø^2$	$ø^2$
Perceived Accessibility	.746	.318	.257	.477	.401	.423	1.000
Perceived security	.720	.214	.204	.430	.401	1.000	
Perceived Usability	.749	.299	.287	.416	1.000		
Loyalty	.711	.245	.249	.1000			

Table 4. Construct reliability and AVE

Variables	**C.R.**	**Fornell & Larcker's AVE**	**Hair et al.'s AVE**
Perceived Accessibility	.983	.938	.680
Perceived Security	.986	.948	.610
Perceived Usability	.990	.963	.712
Loyalty	.990	.962	.730

Next, the structural model was tested by examining the indices for the goodness of fit that include x^2/df, GFI, AGFI, NFI, TLI, CFI, and RMSEA, and the results are as follows: x^2/df = 2.712, GFI = .874, AGFI = .830, NFI = .909, TLI = .928, CFI = .940, and RMSEA = .082. Based upon the overall fit statistics, the proposed structural model can be considered to have a fairly good fit.

Finally, the path coefficients were examined to check the causal effects between the variables. To do so, the significance of the relationships between the variables in the proposed model was analyzed. As predicted in the hypotheses, perceived accessibility had a significant influence on the perceived security ($\beta = .255$, $p < .0001$), perceived security also had a significant influence on the perceived usability ($\beta = .289$, $p < .0001$), and the perceived security was a significant determinant of the loyalty ($\beta = .289$, $p < .0001$). Thus, all of the hypotheses were supported.. Table 5 shows the results of the test of the structural model and Figure 2 below also presents the results of the structural model analyses with R^2 values.

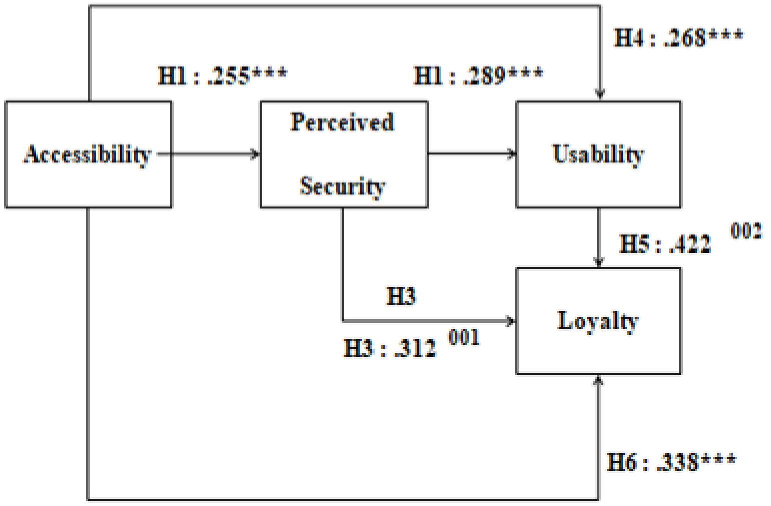

Figure2: Research Model

Table 5. Hypothesis Test

	Paths	**Coeff.**	**Stand. Coeff.**	**P**	**Results**
H1:	Accessibility -> Perceived Security	.255	.271	001	Accept
H2:	Perceived Security -> Perceived Usability	.289	.258	001	Accept
H3:	Perceived Security -> Loyalty	.289	.265	001	Accept
H4:	Accessibility -> Perceived Usability	.268	.357	001	Accept
H5:	Perceived Usability -> Loyalty	.422	.503	002	Accept
H6:	Accessibility-> Loyalty	338	472	001	Accept

Table 6. Varimax Rotation of Four Factor Solution

	Component 1 Perceived Accessibility	Component 2 Perceived Security	Component 3 Perceived Usability	Component 4 Loyalty
ACC1	.822			
ACC2	.901			
ACC3	.900			
ACC4	.891			
SEC1		.747		
SEC2		.856		
SEC3		.838		
SEC4		.835		
USA1			.751	
USA2			.777	
USA3			.817	
USA4			.815	
LOY1				.831
LOY2				.869
LOY3				.829
LOY4				.826
% of Variance	20.14	19.30	17.98	19.48
% of Acc.	20.14	39.44	57.34	76.82

Next, the structural model was tested by examining the indices for the goodness of fit that include x^2/df, GFI, AGFI, NFI, TLI, CFI, and RMSEA, and the results are as follows: x^2/df = 2.712, GFI = .874, AGFI = .830, NFI = .909, TLI = .928, CFI = .940, and RMSEA = .082. Based upon the overall fit statistics, the proposed structural model can be considered to have a fairly good fit.

4. Conclusion

This study empirically investigated the direct and indirect effects of accessibility of mobile banking applications on the perceived cyber security and usability of the applications as well as on user loyalty to the applications and found significant direct and indirect effects. The results emphasize the importance of perceived accessibility and security in understanding the factors that affect user loyalty to mobile banking applications. In other words, the results of this study indicate that mobile banking applications should provide users with highly accessible but secured systems that make it possible for users to process essential transaction-related information and functions quickly, easily, as well as safely. When developing mobile banking applications, developers might consider the findings of this study to improve the perceived quality of security systems and the usability of mobile banking applications, thus improving users' mobile banking experiences and enhancing the usefulness of the applications, as well as making it more likely that users will process their financial transactions with the applications.

In the technology acceptance model (TAM), often employed in information systems and information technology related studies to examine information technology users' behavior, usefulness is one of two important determinants of users' decisions whether or not to adopt technologies [14, 15]. Based on TAM-related prior research, users of mobile banking applications are expected to adopt these applications as online transaction systems. Specifically, when the users of mobile banking applications perceive that the applications are easily accessible, secure, and fully usable, then, the users will think that the applications are useful; accordingly, consumers will not only adopt the applications to use, but also form loyalty to them. However, when they are not satisfied regarding the access to and security of the applications, users will rate the apps' usability as low, which will in turn negatively affect their loyalty to the applications. In sum, one of the interesting findings in this study is that users' perceptions about the security and usability of mobile banking applications were found to be important mediating variables between the applications' accessibility and the users' loyalty to the applications. One of important contributions of this study is the fact that this study not only proposed a research model for cyber security in a mobile banking application context, but also empirically validated the model. In the IS literature, little empirical research has been undertaken on the effects of perceived accessibility and cyber security, which are the main determinants of user loyalty to mobile banking applications in the model. In addition The study also contributes little to our understanding of cyber security strategies for meeting the requirements and expectations of mobile banking application users.

Acknowledgement

The present research was conducted by the research fund of Dankook University in 2017.

References

[1] Bostrom RP, Olfman ,& Sein MK (1990), "The importance of learning style in end-user training," *MIS Quarterly* 3, PP: 101-119.

[2] Black M (1998). "More about metaphor in: Ortony A, editor. *Metaphor and Thought,"* Cambridge: University Press; 1988.

[3] Chu C, & Chan BK (1998), "Evolution of web site design: implications for medical education on the Internet," *Computer in Biology and Medicine* 28, Pp: 470-472.

[4] Fornell, C, & Larcker, D.F (1981), "Evaluating Structural Equation Models with unobservable variables and measurement error," *Journal of Marketing Research*, 18, pp: 39-50.

[5]George, B. (2012), "The Problem with Survey Research, New Brunswick, NJ: Transaction, P. 15.

[6] Hair, JF, & Black WC, Babin B.J, Anderson, RE, & Tatham R.L(2006) Multivariate data nalysis, 6th ed., Prentice-Hall International, 2006.

[7] Jacobs, S. (1999). "Section 255 of the Telecommunications Act of 1996: Fueling the Creation of New Electronic Curbcuts".

[8] Kassim N, & Abdullah NA (2010), "The Effect of Perceived Service Quality Dimensions on Consumer Satisfaction, Trust, and Loyalty in e-Commerce Settings," *Asia Pacific Journal of Marketing and Logistics* 22, pp.351-371.

[9] Lee FH & Wu WY (2011), "Moderating Effects of Technology Acceptance Perspective on e-Service Quality Formation," *Expert Systems with Applications* 2011: 38, p.7766-7773.

[10] McWilliam G & Dumas A (1997), "Using metaphor in new brand design," *Journal of Marketing Management* 1997:13: p. 265-284.

[11] Morley D & Parker CS (2011), "Understanding computers: today and tomorrow comprehensive," Cengage Learning; 2011.

[12] Moran T (1981), "An applied psychology of the use," *ACM Computing Surveys* 1981:13: p. 1-12.

[13] Moshagen M & Thielsch MT (2010), "Facets of visual aesthetics," *International Journal of Human-Computer Interaction* 68,689-709.

14] Ransbotham S & Mitra S (2009), "Choice and change: a conceptual model of paths to information security compromise," *Information Systems Research* 1,121-139.

[15] Rouse WB & Morris NM (1986), "On looking into the black box: prospects and limits in the search for mental models," *Psychological Bulletin* 100, 349-363.

[16] Schmidt KE, Liu YL, & Sridharan S (2009), "Webpage aesthetics, performance, and usability: design variables and their effects," *Ergonomics* 2009,52, 641-643.

[17] Szajna B (1996), "Empirical evaluation of the revised technology acceptance model," *Management Science* 42, 85-92.

18] Wang RY & Strong DM (1996), "Beyond accuracy: what data quality means to data consumers. Journal of Management Information Systems," 12, 5-34.

[19] Wolfe CR (2001), "Plant a tree in cyberspace: metaphor and analogy as design elements in web-based learning environments," *Cyber Psychology and Behavior*, 4,67-76.

[20] AIRC (2008), Attack Intelligence Research Center annual threat report: "2008 overview and 2009 predictions," Attack Intelligence Research Center, Aladdin Knowledge Systems, Belcamp, MD (accessed 2008 online at: http://www.aladdin.com/pdf/airc/AIRC-Annual- Threat-Report2008.pdf).

[21] Anderson, E W, Fornell C, & Lehmann D R (1994), "Customer Satisfaction, Market Share, and Profitability: findings from Sweden," Journal of Marketing, 58, 53−-66.

[22] Asubonteng, P, McCleary, K J, & Swan, J E (1996), "SERVQUAL Revisited: a Critical Review of service quality," *The Journal of Services Marketing*, 10, 62-81.

[23] Bailey, JE & Pearson, S W (1983), "Development of a Tool for Measuring and Analyzing Computer User Satisfaction," *Management Science*, 29, 530–545.

[24] Baroudi, J, & Orlikowski, W. (1988), "A short-form measure of user information Satisfaction: a psychometric evaluation and notes on use," *Journal of Management Information Systems*, 44–59.

[25] Bart Y, Shankar V, Sultan F, & Urban, G (2005), "Are the drivers and role of online trust the same for all web sites and customers? a Large-scale exploratory empirical Study," *Journal of Marketing*, 69, 133–152.

[26] Berinato S (2006), "The Global State of Information Security 2005," Available online at: http://www. csoonline.com/read/100105/servey.html (accessed 16 April 2006).

[27] Boss SR, & Kirsch, LJ, "The last line of defense: motivating employees to follow corporate security guidelines," in *Proceedings of the 28th International Conference on Information Systems,* Montreal, December, 2007, pp. 9-12.

[28] Bulgurcu, B., Cavusoglu, H., & Benbasat, I (2010), "Information security policy compliance: an empirical Study of rationality-based beliefs and information security awareness," *MIS Quarterly*, 34, 523-548.

[29] Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004), "Economics of IT security management: four improvements to current security practices," *Communications of the Association for Information Systems,* 14, 65-75.

[30] Cavusoglu, H., Son, JY, & Benbasat, I. (2009), "Information security control resources in organizations: A Multidimensional View and Their Key Drivers," working paper, 2009, Sauder School of Business, University of British Columbia.

[31] Cavusoglu, H., Mishra, B., and Raghunathan, S., "A Model for Evaluating IT Security Investments," *Communications of the ACM,* Vol. 47, No. 7, 2004b, pp. 87-92.

[32] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Effects of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers." *International Journal of Electronic Commerce,* Vol. 9, No. 1, 2004c, pp. 69-104.

[33] Choi, J. and Lee, H., "Facets of Simplicity for the Smartphone Interface: A Structural Model," *International Journal of Human-Computer Studies*, Vol. 70, 2012, pp. 129-142.

[34] Cronin, J.J., Looking Back to See Forward in Services Marketing: Some Ideas to Consider," *Managing Service Quality*, Vol. 13, No. 5, 2003, pp. 332-337.

[35] Cronin, J.J., Brady, M.K., and Hult, G.T.M, "Assessing the Effects of Quality, Value, and Custoemr Satisfaction on Consumer Behavioral Intentions in Service Environments," *Journal of Retailing,* Vol. 76, No. 2, 2000, pp. 193-218.

[36] DeLone, W.H., and McLean, E.R., "Information Systems Success: The Quest for The Dependent Variable," *Information Systems Research,* Vol. 3, No. 1, 1992, pp. 60-95.

[37] DeLone, W.H., and McLean, E.R., "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems,* Vol. 19, No. 4, 2003, pp. 9-30.

[38] Doherty, N.F. and Fulford, H., "Aligning the Information Security Policy with the Strategic Information Systems Plan," *Computers and Security*, Vol. 25, No. 1, 2006, pp. 55-63.

[39] Doll, W. J. and Torkzadeh, G., "The Measure of End-User Computing Satisfaction," *MIS Quarterly,* Vol. 12, No. 2, 1988, pp. 259–274.

[40] Dube, L. and Maute, M., "The Antecedents of Brand Switching, Brand Loyalty and Verbal Responses to Service Failure," *Advances in Services Marketing and Management,* Vol. 5, 1996, pp. 127–151.

[41] Ernst & Young, "Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey" (accessed 2008 at http://www.ey.com/Publication/vwLUAssets/ 2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles,pdf).

[42] Flint, D.J., Blocker, C.P., and Boutin, P.J., "Customer Value Anticipation, Customer Satisfaction and Loyalty: An Empirical Examination," *Industrial Marketing Management,* Vol. 40, 2011, pp. 219-230.

[43]Fornell, C. and Larcker, D.F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, Vol. 18, 1981, pp. 39-50.

[44] Ghosh, S., Surjadaja, H., and Antony, J., "Optimizaiton of the Determinants of E-service Operations," *Business Process Management Journal*, Vol. 10, No. 6, 2004, pp. 616-636.

[45] Gilbert, L.A. and Han, H., "Understanding Mobile Data Services Adoption: Demography, Attitudes or Needs?" *Technological Forecasting and Social Change,* Vol. 72, 2005, pp. 327-337.

[46] Gorden, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R., 2006 CSI/FBI Computer Crime and Security Survey. Available online at: http://www.gocsi.com (accessed 9 January 2007).

[47] Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., and Tatham, R.L., *Multivariate Data Analysis,* 6th ed., Prentice-Hall International, 2006.

[48] Hassel, L. and Wiedenbeck, S., *Human Factors and Information Security*, DIMACS Workshop on Usable Privacy and Security Software, 7-8 July 2004, DIMACS Centre, CORE Buildoing, Rutgers University, Piscataway, NJ.

[49] Ho, C.T.B. and Lin, W.C., "Measuring the Service Quality of Internet Banking: Scale Development and Validation," *European Business Review*, Vol. 22, No. 1, 2010, pp. 5-24.

[50] Huang, D.L., Rau, P.L.P., and Salvendy, G., "Perception of Information Security," *Behavior and Information Technology,* Vol. 29, No. 3, 2010, pp. 221-232.

[51] Jih, W.J., Wong, S.Y., and Chang, T.B., "Effects of Perceived Risks on Adoption of Internet Banking Services: An Empirical Investigation in Taiwan," *International Journal of e-Business Research,* Vol. 1, 2005, pp. 70-88.

[52] Jung, W (2018), The Effects of the Perceived Accessibility and Cyber Security of Mobile Banking Applications on User Loyalty to the Applications, "*International Journal of Mobile Device Engineering*, 2, 7-12.

[53] Shaughnessy, J.; Zechmeister, E.; Jeanne, Z. (2011). *Research methods in psychology* (9th ed.). New York, NY: McGraw Hill. pp. 161–175.