Vol. 6, No. 1, June 2015 (pp. 27-43)
https://imr.kangwon.ac.kr/apjb.6.1.201506.27.
ISSN 2233-5900 (Print)
ISSN 2384-3934 (Online)

The effect of security factors on the continuance of Internet banking usage among Malaysians

Normalini, M.K.[a]

Senior Lecturer, School of Management, Universiti Sains Malaysia, 11800 Minden, Penang, Malaysia

Contents

Abstract

The objective of the present study is to identify the security factors that influence customer trust towards intention to continue using Internet banking in Malaysia. The participants are individual Internet banking users in Peninsular Malaysia. Data was collected through self-administered questionnaires distributed using the drop-off and pick-up (DOPU) technique to bank branch managers who then passed the questionnaires to their customers. A total of 413 respondents completed the questionnaires. The SPSS statistical analysis software package and Partial Least Squares statistical method were used for data analysis and hypothesis testing. The results show that authentication, confidentiality, data integrity and non-repudiation are significant factors that influence customer trust towards intention to continue using Internet banking. Trust plays a critical role in influencing the intention to continue using Internet banking in Malaysia while perceived privacy does not. An understanding of the factors identified in this study will enable Internet banking providers to effectively and efficiently enhance the security of services and thereby promote continued usage of Internet banking among customers. The findings of this study are thus expected to be of great use to Internet banking providers as improvements in Internet banking security will increase business in the long run.

Keywords: Perceived Privacy, Authentication, Non-repudiation, Integrity, Confidentiality, Trust, Internet banking

• Received 30 March 2015, Revised 20 June 2015, Accepted 25 June 2015

[a] E-mail: normalini_mk@yahoo.com

Ⅰ. Introduction

Internet banking security concerns are prevalent owing to threats arising from internet networks and electronic transactions. Authentication failures in internet systems lead to unauthorized account access and retrieval of personal financial information, creating anxiousness among customers using Internet banking services. Online banking service providers, recognizing customer security needs, are beginning to utilize a number of technologies that have been developed to ensure the security of electronic transactions. However, the safety and security of these transactions remain a concern for Internet banking customers (Sathye, 1999).

A study conducted in Australia found that the key impediments to customer adoption of Internet banking were security concerns and the lack of familiarity with Internet banking (Sathye, 1999). Many similar studies conducted in Malaysia and other countries have examined trends in adoption of Internet banking and causes of delayed growth. Security and personal preference factors are among the reasons found to hinder the growth and adoption of Internet banking in Malaysia (Suganthi, Balachandher, & Balachandran, 2001).

By just reading the signals, following the trends and issues on security would not be everything for Internet banking. Internet banking crimes keep increasing by the day. Considering the importance of security in online banking transactions, the key security factors influencing customer intention to continue using Internet banking is investigated in this study. Therefore, the findings from this research could provide important suggestions as to the extent of enhancement that could be done on the level of security in Internet banking.

Ⅱ. Literature Review

Internet banking adoption by Malaysian banking customers from the two leading banks offering such services in 2002, Maybank and HSBC, amounted to approximately 25,000 and 10,000 customers respectively (Yu, 2002). However, there is generally little acceptance of Internet banking among Malaysians and the main determining factors for the adoption of these services in Malaysia have not been studied comprehensively (Ndubisi & Sinti, 2006). Although financial institutions have embarked on diverse tactics to attract users, the continued low rates of Internet banking adoption in Malaysia, a developing country, is supported by findings from Jano et al. (2012) and Raman et al. (2008). Furthermore, Internet banking usage in Malaysia does not correspond to the growth of Internet banking services, even with the range of benefits that can be obtained from such services (Mohan et al., 2013; Mozie, Mustapha and Ghazali, 2012). Hence, the diffusion of Internet banking in Malaysia is still at an early phase even though the electronic transformation of other services is well underway. Increasing Internet banking adoption levels among customers has been especially challenging for the banking industry as there is limited Internet banking research conducted in Malaysia to identify areas of improvement and facilitate widespread acceptance (Ndubisi & Sinti, 2006).

In order to accelerate the adoption of Internet banking in Malaysia, the basic principles of safety and security need to be embedded in online banking processes and systems. Based on previous research, essential security factors required for e-commerce can be summarized into five categories: authentication, non-repudiation, confidentiality, privacy and data integrity. Authentication is the procedure of guaranteeing that trading parties in an electronic transaction or communication are who they claim to be. Non-repudiation refers to the method of ensuring that trading parties are not able to deny having participated in a transaction after it is completed. Confidentiality is the term associated with the assurance that all communications between trading parties are restricted to the parties involved in the transaction. Maintaining confidentiality during the online banking process is essential due to the risk of hackers obtaining sensitive information from customers. Privacy protection is an absolutely critical part of maintaining confidentiality and is the guarantee that personal information about customers collected from their electronic transactions is protected from disclosure without permission. Data integrity refers to the assurance that there is neither creation of false data in a transaction nor illicit interception, modification or deletion of transmitted data (Suh & Han, 2003).

1. PERCEIVED PRIVACY

Consumer privacy, as termed by Goodwin (1991), is "the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behaviour, and (b) dissemination of information related to or provided during such transactions or behaviours to those who were not present". Perceived privacy on the other hand, is defined by Yousafzai et al. (2003) as the "customer's perception regarding their ability to monitor and control the information about themselves".

Trust stemming from perceived privacy can most likely be reached by letting the balance of power shift towards greater collaborative interaction between online businesses and their customers (Hoffman and Novak, 1997, as cited in Hoffman, Novak and Peralta, 1999). The balancing of power to obtain trust involves, among other things, the recognition of a consumer's right to data ownership during online transactions. Hoffman, Novak and Peralta (1999) found that trust issues derive from the perceived lack of control over a consumer's personal information and the access others have to the information during the online navigation process. There is thus an implication that confidentiality, an important aspect of building trust, can possibly be lost in such online processes (Culnan & Armstrong, 1999).

2. AUTHENTICATION

Distinct usernames, PINs), passwords, and preferred security questions and answers are among the tools or access codes used to verify the identity of customers. These tools operate as keys to obtain access to customers' personal accounts and financial information as well as banking facilities, products and services offered via the online banking system. Customers are advised to maintain the confidentiality of their personal codes by not sharing or providing easy access to them in order to preserve the integrity of access codes.

3. CONFIDENTIALITY AND DATA INTEGRITY

Banks utilize a fusion of authentication, encryption and auditing mechanisms to provide assurance that there is safeguarding of the privacy, confidentiality, and integrity of transactions and information that is exchanged, disclosed, shared, stored or used in online banking systems. The combinations of these mechanisms function as a formidable barrier to guard against the penetration and abuse of systems in any form. Among the mechanisms used are:

- secure sockets layer (SSL) channel
- 128-bit Encryption
- username & password protection and authentication
- firewalls, and
- account-locking

Series of independent security audits are conducted to ensure that all mechanisms are systematically tested to protect and safeguard against known security issues and prevent any form of tampering or theft of information or threats to transactions.

4. NON-REPUDIATION

Logs of transactions are maintained and regularly updated by banks and record a variety of information including the nature, time, and date of transactions that have been entered into by customers. These records enable the verification of all types of completed transactions and provide the proof needed should any issue ever arise.

5. TRUST

Social psychologists defined trust as an expectation about the behaviour of others in transactions, focusing on the contextual factors that enhance or inhibit the development and maintenance of trust (Lewieki & Bunker, 1995). According to Mayer, Davis, and Schoorman (1995) and Rousseau, Sitkin, Burt, and Camerer (1998), customer's trust on electronic banking is defined as, "a psychological state which leads to the willingness of customer to perform banking transactions on the Internet, expecting that the bank will fulfil its obligations, irrespective of customer's ability to monitor or control bank's actions".

6. Intention TO CONTINUE USE

Behavioural intention measures a person's relative strength of intention to display a specific behaviour. It is likely that a person will adopt a specific behaviour if he or she intends to do so. This implies that behavioural intention (BI) to continue using internet banking is expected to have a positive influence on users' interaction with online banking systems.

Ⅲ. Theoretical Framework

Information security encompasses not only technical issues but also human factors and is an ever increasing problem that is becoming a key cause of fear among computer users. Even though there are almost an uncountable number of threats to information security, this number is unfortunately on the rise. For the average person using the Internet, information security may mean among other things, working with computers without being attacked by viruses, conducting online transactions with the assurance that credit card information will not be subject to theft and browsing e-mails without receiving unsolicited or undesired electronic messages (Huang, Rau and Salvendy, 2007).

In Malaysia, weak security and Internet banking application trustworthiness are the central issues related to Internet banking (Normalini and Ramayah, 2015). Therefore, this study will investigate privacy and security dimensions that influence the intention to continue using Internet banking applications and users' trust in Internet banking.

1. Model of Trust

Customers trading in the e-commerce world face a variety of challenges and among the major issues faced is the problem of security which is caused by vulnerabilities found in the Internet, the foundation of e-commerce (Hussin, Dahlan, and Bahari, 2009). When customers conduct transactions on the Internet, anyone from anywhere in the world may be able to access the information being transferred. As there are constantly increasing number of ways to penetrate security mechanisms, the risk of information theft, transaction tampering and corruption of data could become a reality. If security breaches occur, customers may incur damages ranging from privacy invasion to financial loss (Suh & Han, 2003). Many researchers have discussed basic security principles that are crucial for e-commerce (Aldridge, White, & Forcht, 1997; Bhimani, 1996; Furnell & Karweni, 1999; Gefen, 2000; Ratnasingham, 1998). In Internet banking, prior research has classified these into five categories: authentication, non-repudiation, confidentiality, data integrity and privacy.

Ⅳ. Research Methodology

1. Research Model

The primary participants are Internet banking users in Peninsular Malaysia (Such as Penang, Selangor, Kuala Lumpur and Johor). Data comes from personal Internet banking users who perform banking transactions via Internet banking. Data collection of this study was through a self-administered questionnaire. In this research, drop-off and pick-up (DOPU) technique was employed. The questionnaires were distributed through this method to the respective bank branch managers which were willing to distribute to their customers. A total of 413 respondents completed the questionnaires as requested. The questionnaire consisted of 2 sections. The first section collected the demographic data, the second section elicited information about perceived risk dimensions, perceived ease of use, perceived usefulness, attitude and intention to continue using Internet banking. The sampling method used in this research is purposive sampling because this method is confined to specific types of people who can provide the desired information which are Internet banking users.

The influence of privacy and security on users' acceptance of e-banking services has been supported by several authors (Sathye, 1999; Poon, 2008). Based on the five basic security factors identified for Internet banking, this study constructed a theoretical framework which can be found in Figure 1. To test the framework, six hypotheses were proposed to understand the relationship between the security factors and the trust customers have in Internet banking as well as to find out the impact of trust on customers' intention to continue using Internet banking.

The hypotheses were proposed based on research conducted by several authors who can be found in Table 1. The following are the hypotheses that were proposed and tested:

H1 : Perceived privacy has a positive impact on the customer's trust in Internet banking.

H2 : Authentication has a positive impact on the customer's trust in Internet banking.

H3 : Confidentiality has a positive impact on the customer's trust in Internet banking.

H4 : Data Integrity has a positive impact on the customer's trust in Internet banking.

H5 : Non-repudiation has a positive impact on the customer's trust in Internet banking.

As the level of ambiguity in virtual environments make users especially susceptible to threats, trust in e-services like Internet banking is essential aspect for users conducting transactions online (Roca, Garcia, & de la Vega, 2009). Trust in not only e-services but also service providers is important as Bhattacherjee (2002) found that trust has a positive effect on an individual's willingness to conduct transactions with an online bank. Therefore it is proposed that:

H6 : Trust has a positive impact on the customer's behavioural intention to continue using Internet banking.

Fig. 1. Research Framework

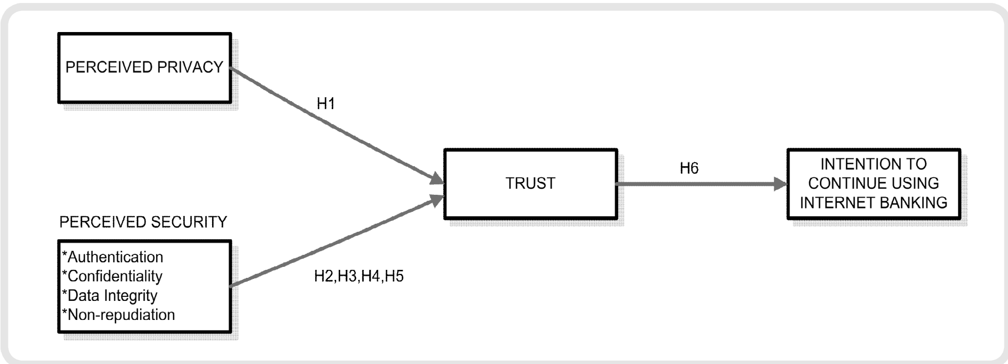

Table 1: Research Hypotheses

Hypotheses	Source
H1: Perceived privacy has a positive impact on the customer's trust in Internet banking.	Featherman & Pavlou, 2003
H2: Authentication has a positive impact on the customer's trust in Internet banking	Suh & Han, 2003
H3: Confidentiality has a positive impact on the customer's trust in Internet banking.	Suh & Han, 2003
H4: Data Integrity has a positive impact on the customer's trust in Internet banking	Suh & Han, 2003
H5: Non-repudiation has a positive impact on the customer's trust in Internet banking	Suh & Han, 2003
H6: Trust has a positive impact on customer's behavioural intention to continue using Internet banking	Suh & Han, 2003; Yousafzai et al.,2009; Bhattacherjee, 2001; Chung & Skibniewski, 2007

2. Population and Sampling

The population for this study consisted of Internet banking users from Malaysia. A non-probability sampling technique, specifically purposive sampling, was used for this study. Data was collected using self-administered q uestionnaires that were circulated to respondents using the drop-off and pick-up (DOPU) technique. There were a total of 413 usable responses which were retrieved from bank branch managers who had helped to distribute and collect the questionnaires from their Internet banking customers. The measures were all adapted from published literature (see Table 2).

Table 2: Questionnaire Items Used in This Study

Constructs	Questionnaire Items	Source
Perceived Privacy	Internet hackers (criminals) might take control of my checking account if I used Internet Banking What are the chances that using Internet Banking will cause you to lose control over the privacy of your payment information? My signing up for and using an Internet Banking lead to a loss of privacy for me because my personal information would be used without my knowledge.	(Featherman & Pavlou, 2003)
Authenti-cation	The transactions I send are transmitted to my Internet banking site. The messages I receive are transmitted from my Internet banking site. My Internet banking site ascertains my identity before sending any messages to me. My Internet banking site ascertains my identity before processing the transaction received from me.	(Suh & Han, 2003)
Confi-dentiality	All the communication with my Internet banking site are strictly within the site and me. I am convinced that my Internet banking site respects the confidentiality of the transactions received from me. My Internet banking site uses some security controls for the confidentiality of the transactions. My Internet banking site checks all communications between the site and me for the protection from wiretapping or eavesdropping.	(Suh & Han, 2003)
Data Integrity	My Internet banking site checks the information communicated with me for accuracy. My Internet banking site takes steps to make sure that the information in transit is accurate. My Internet banking site takes steps to make sure that the information in transit is not deleted. My Internet banking site devotes time and effort to verify the accuracy of the information in transit.	(Suh & Han, 2003)
Non-Repudiation	My Internet banking site will not deny having participated in a transaction after processing it. My Internet banking site will not deny having sent me a message. My Internet banking site will not deny having received a transaction from me. My Internet banking site provides me with some evidence to protect against its denial of having received a transaction from me.	(Suh & Han, 2003)
Trust	My Internet banking site is trustworthy. My Internet banking site keeps its promises and commitments. I trust my Internet banking site. I trust my bank.	(Suh & Han, 2003; Yousafzai et al., 2009)
Intention	I intend to continue using Internet banking services rather than discontinue its use. My intentions are to continue using Internet banking services than use any alternative means (traditional banking). If I could, I would like to discontinue my use of Internet banking services. I intend to continue using Internet banking services whenever I need it. I intend to continue using Internet banking service feature since it is good.	(Bhattacherjee, 2001; Chung & Skibniewski, 2007)

Ⅴ. FINDINGS

1. Demographic Profile

The questionnaire consisted of two separate sections. The first section was designed to collect demographic data and the second section elicited information about perceived privacy, authentication, confidentiality, data integrity, non-repudiation, trust and intention to continue using Internet banking. The sampling method used in this research was purposive sampling because the method targets specific types of people who can best provide the desired information for the study, namely Internet banking users.

Table 3 presents the demographic data for the 413 respondents who were Internet banking users in Malaysia. The data includes variables such as gender, age, race,

Table 3: Profile of Internet Banking Respondents

Demographics	Categories	Frequency	%
Gender	Male	171	41.4
	Female	242	58.6
Age	< 20	1	0.2
	20-29	132	32.0
	30-39	192	46.5
	40-49	64	15.5
	>50	24	5.8
Race	Malay/ Bumiputra	298	72.2
	Chinese	71	17.2
	Indian	35	8.5
	Others	9	2.2
Highest Academic	SPM or equivalent	51	12.3
	STPM or equivalent	23	5.6
	Certificate/Diploma	66	16.0
	Degree	180	43.6
	Post-Graduate	93	22.5
Occupation	Professional	216	52.3
	Housewife/Husband/Self-employed	11	2.7
	Clerical Staff	65	15.7
	Technical Staff	42	10.2
	Others (Please specify)	78	18.9
	Missing	1	0.2
Total years of working experience	<1 year	1	0.2
	1-10 years	242	58.6
	11-20 years	135	32.8
	21-30 years	23	5.5
	>30 years	12	2.8
Total years of Internet usage	1-10 years	273	66.1
	11-20 years	133	32.3
	21-28 years	7	1.60
Total years of Internet banking	<3 years	111	26.8
	3-6 years	212	51.3
	7-11 years	90	21.9

highest academic qualification, occupation, working experience (total number of years), total number of years of internet usage, and total number of years of internet banking usage.

The majority of respondents were young and middle aged adults, with almost 78.50 percent within the range of 20 to 39 years old. As expected, the respondents were highly educated and the majority of them had academic qualifications, namely, certificates or diplomas (16%), degrees (43.6%) and postgraduate qualifications (22.5%). The majority of respondents (72.2%) were of Malay or Bumiputra ethnicity. Respondents mostly categorised themselves as professionals (52.3%) while 18.9 percent of respondents held executive level positions and placed themselves under the category of “others” (e.g. marketing executive, auditor, bank executive, finance officer, HR officer). Almost all respondents had work experience and most of them had worked for at least 1 to 20 years (91.40%). The fact that 98.40% of respondents had used the Internet for a period of 1 to 20 years suggests that most of them could have needed access to the Internet for work. However, 78.10% of respondents had only used Internet banking for a period of 0 to 6 years.

2. Analysis

To analyse the data collected, the partial least squares (PLS) approach was used. The Smart PLS 3.0 software (Ringle, et al., 2014) and two-step analysis approach, as suggested by Anderson and Gerbing (1988), was employed to analyse the data. In addition, following the suggestions of Chin (1998), the bootstrapping method (500 resamples) was applied to determine the significant levels for loadings, weights and path coefficients.

3. Measurement Reliability And Validity

Composite reliabilities of the latent variables (Fornell and Larcker, 1981) were higher than 0.80, and in general close to the value of 0.90, showing a high internal consistency of indicators measuring each construct and thus confirming construct reliability. The average variance extracted (AVE) was also higher than 0.60, indicating that the variance captured by each latent variable was significantly larger than the variance due to measurement error, thus demonstrating unidimensionality and a high convergent validity of the constructs. Reliability and convergent validity of the measurement model was also confirmed by computing standardized loadings for indicators (Table 4) and Bootstrap t-statistics to assess their significance (Anderson and Gerbing, 1988). All standardized loadings exceeded the 0.6 threshold, thus confirming a high convergent validity of the measurement model. Two items, PP2 and INT3, were deleted due to low loadings.

Discriminant validity was assessed by determining whether the shared variance of each latent variable with its own measurement variables was higher than with other constructs (Fornell and Larcker, 1981; Fornell and Bookstein, 1982). This was computed by comparing the correlations between constructs and each constructs’ squared root of AVEs (Gholami et al., 2013). The square root of the average variance extracted (AVE) exceeded the inter-correlations of the construct with the other constructs in the model, indicating adequate discriminant validity. As shown in Table 5, all the squared roots of AVEs for constructs were higher than the correlation values in their respective rows and the columns indicating adequate discriminant validity (Fornell & Larcker, 1981).

Table 4: Results of the Measurement Model

Construct	Item	Loadings	AVE	CR
Perceived Privacy	PP1	0.679	0.726	0.836
	PP3	0.995		
Authentication	PA1	0.903	0.852	0.958
	PA2	0.917		
	PA3	0.943		
	PA4	0.928		
Confidentiality	PCON1	0.917	0.856	0.960
	PCON2	0.937		
	PCON3	0.938		
	PCON4	0.910		
Data Integrity	PDI1	0.941	0.889	0.970
	PDI2	0.953		
	PDI3	0.938		
	PDI4	0.940		
Non Repudiation	PNR1	0.928	0.890	0.970
	PNR2	0.956		
	PNR3	0.955		
	PNR4	0.934		
Trust	TRUST1	0.920	0.869	0.964
	TRUST2	0.942		
	TRUST3	0.950		
	TRUST4	0.916		
Intention to continue using IB	INT1	0.944	0.860	0.961
	INT2	0.897		
	INT4	0.942		
	INT5	0.925		

Notes: PP2 and INT3 were deleted due to low loadings

Table 5: Discriminant Validity of Constructs

	PA	PCON	PDI	INT	PNR	PP	TRUST
Authentication	0.923						
Confidentiality	0.757	0.925					
Data Integrity	0.749	0.856	0.943				
Intention	0.593	0.637	0.635	0.927			
Non Repudiation	0.643	0.691	0.703	0.535	0.943		
Perceived Privacy	0.050	0.032	0.036	-0.005	0.063	0.852	
Trust	0.619	0.672	0.672	0.760	0.579	-0.013	0.932

Notes: Diagonal elements are the square root of average variance extracted (AVE) between the constructs and their measures. Off-diagonal elements are correlations between constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements in the same row and column.

4. Structural Model

Structural models show the causal relationships among constructs in the models (path coefficients and the R^2 value). Together, the R^2 value and path coefficients (beta and significance) indicate how well the data supports and hypothesises a model (Chin 1998; Sang et al. 2010; Ramayah et al., 2011). Table 6 and Figure 2 show the results of the structural model from the PLS output for this study. It was found that four security factors were positively related to Trust, including Authentication (R^2 = 0.511, β = 0.166, p< 0.01), Confidentiality (R^2 = 0.511, β = 0.246, p < 0.01), Data Integrity (R^2 = 0.511, β = 0.246, p < 0.01), and Non-repudiation (R^2 = 0.511, β = 0.133, p < 0.05). It was also found that Trust was positively related to Intention (R^2 = 0.578, β = 0.760, p < 0.01). As such, the findings supported H2, H3, H4, H5 and H6 of this research. As Perceived Privacy (β = - 0.046, p> 0.05) was not a significant predictor of Trust, H1 was not supported. Trust explained 57.8% of the variance in Intention. More in-depth analysis revealed that the most important predictors of intention were trust, authentication, confidentiality, data integrity and non-repudiation.

The Q^2 value, which measures predictive relevance, was subsequently tested in the study via the blindfolding procedure. Part of the data for a particular block of indicators is omitted during parameter estimations in this procedure and the omitted data is then estimated using estimated parameters (Chin, 2010). Chin (2010) suggested that an omission distance of 5 to 10 was acceptable as long as the sample size was large. As proposed by Fornell and Cha (1994), a Q^2 > 0 implies that the model has predictive relevance whereas a Q^2 < 0 represents a lack of predictive relevance. Using the blindfolding procedure, the cross validated communality (cv-comm) and cross validated redundancy (cv-red) can be calculated. However, the cr

Fig. 2. Hypothesis Testing Results

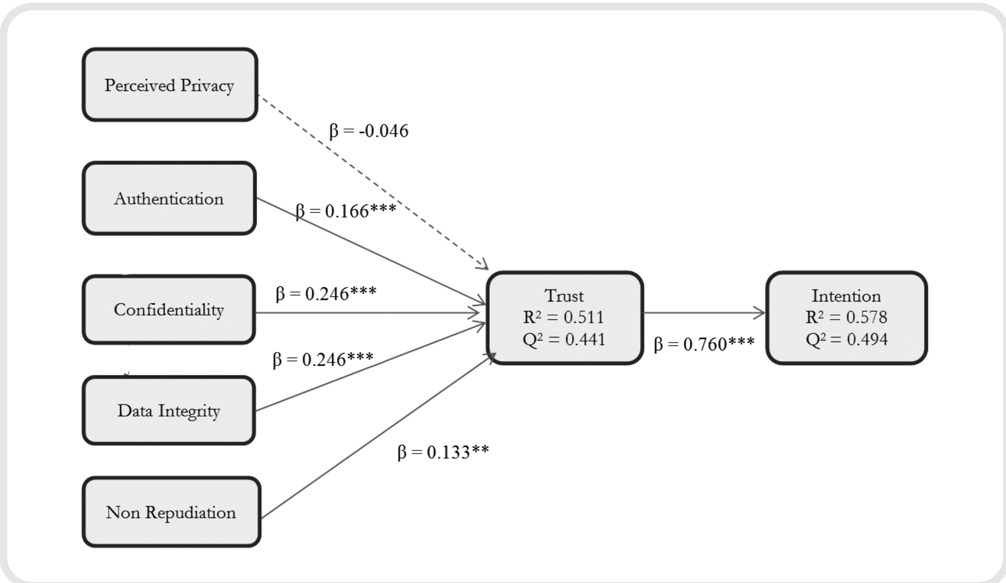

Table 6. Hypothesis Testing

Hypothesis	Relationship	Beta	Std Error	t-value	Decision
H1	PP → TRUST	-0.046	0.046	0.991	Not Supported
H2	PA → TRUST	0.166	0.066	2.524**	Supported
H3	PCON → TRUST	0.246	0.101	2.445**	Supported
H4	PDI → TRUST	0.246	0.099	2.472**	Supported
H5	PNR → TRUST	0.133	0.058	2.266*	Supported
H6	TRUST → INT	0.760	0.038	19.970**	Supported

Notes: **p<0.01(2.33), *p<0.05(1.645); (based on the one-tailed test)

oss-validated redundancy measure can be further used to examine the predictive relevance of a theoretical/structural model (Chin, 2010). Thus, the cross validate redundancy for 2 endogenous constructs, Trust and Intention to continue using Internet banking, was calculated in this study (see Figure 1). The Q^2 values obtained were 0.441 and 0.494 respectively, indicating that the model has predictive relevance.

Ⅵ. DISCUSSION

This research has used the model of e-trust banking (Yousafzai et al., 2003) as the basis for information system (IS) acceptance. The rationale for causal relationships has been developed in the model based on combined theoretical frameworks. The model incorporates the main dimensions of security to identify factors that influence intention to continue using Internet banking; namely perceived privacy, perceived security dimensions and trust.

Mukherjee and Nath (2007) stated that the privacy and security features of websites along with shared values are key antecedents of trust, which in turn positively influence the behavioural intentions of customers. The development of trust affected the intention to conduct transactions and trust was particularly influenced by consumers' perceived security related to the handling of their personal data (Flavián and Guinalíu, 2006). Unexpectedly, this research has found that perceived privacy has an insignificant impact on customers' trust in Internet banking. An explanation of this finding might be that Internet banking customers in Malaysia have the perception that other issues such as security is more important and serious compared to privacy issues. According to Kim, Steinfield, and Lai (2008), empirical evidence shows that security protection mechanisms are more important in affecting consumers' behaviour than privacy. Another possible explanation is that the strong privacy policies which are enforced by the Internet banking providers create customer confidence in Internet banking. The results of the descriptive analysis for customers' demographics (Table 3) clearly show that the majority of the respondents were experienced Internet banking users since those with Internet banking experience above 3 years was 73.2% (combined total of 51.30% for 3 to 6 years of experience and 21.90% for 7 to 11 years of experience). A possible explanation is that experienced Internet banking customers are more familiar with the security related technology as they easily recognize features such as security certificates or encryption keys. Given that these security characteristics guarantee almost total privacy, the relative importance of privacy concerns for these users is comparatively lower. Thus, the trust in Internet banking with the presence of security features eases the decision to disclose personal and financial information. Therefore, Perceived Privacy would not influence customers' trust in Internet banking.

On the other hand, authentication has been proved to have a significant positive impact on customers' trust associated with the use of Internet banking. The rational justification of this finding might be that once the perceived strength of authentication is high, an increased level of customers' trust in using Internet banking is then possible. Furthermore, it has also been found that confidentiality has a significant positive impact on customers' trust associated with the use of Internet banking. It can be concluded that confidentiality might facilitate the development of trust even more so as the foundations of trust in banking usually require accurate and reliable information.

Consequently, this study supports the important role of data integrity as a significant determinant of customers' trust and intention to continue using Internet banking. Therefore, it can be concluded that data integrity might facilitate the development of trust since data in transmissions are not created, intercepted, modified, or deleted illicitly. It has also been proven that non-repudiation has a positive impact on the customers' trust in Internet banking. The explanation for this is obvious as once the perception of non-repudiation is high, Internet banking customers would have increased trust associated with higher levels of intention to continue using Internet banking.

In this study, it has been proven that trust has a significant positive impact on intention to continue using Internet banking. In other words, a high level of trust in Internet banking may increase the level of intention to continue using Internet banking. The rational justification of this conclusion might be that once Internet banking customers in Malaysia have confidence in the reliability of Internet banking, they might have positive feeling about conducting banking transaction online via the use of Internet banking.

Ⅶ. Theoretical And Practical Implications

The contributions of this research can be appreciated from two perspectives: theoretical and practical. By using a model on e-trust banking (Yousafzai et al., 2003), this research may help to enhance and deepen the understanding of the model by applying it to Internet banking and incorporating factors that affect intention to continue using Internet banking. Rationale for causal relationships in the model have been developed based on combined theoretical frameworks, providing further insights on factors influencing adoption of Internet banking. In addition, this study adds to literature by providing an in-depth understanding of the characteristics of perceived security and its influence on Internet banking usage by investigating a multi-dimensional construct of security (namely: Authentication, Confidentiality, Data Integrity and Non-repudiation).

Several important implications arise from the results of this study. The results from this research identify factors that impact the customers' intention to continue using

Internet banking in Malaysia and thus provide important and comprehensible insights for practitioners in the banking industry. The outcome of this study is crucial as it can lead to greater awareness among banking institutions in Malaysia about the importance of security and trust in Internet banking. The answers provided by this study hold the key to enhancing the level of security in Internet banking and could also help banks to devise strategic marketing strategies that promote online banking applications in the future.

Ⅷ. Suggestions For Future Research

Future research on the topic of Internet banking in Malaysia should be extended to a wider geographical area. This will enable research results to become a greater representation of the Internet banking environment in Malaysia compared to results from only one or a few regions. Besides that, respondents from different countries can be surveyed and cross-cultural comparisons carried out. Larger samples can also be used in future studies to improve the accuracy and reliability of research findings. The method of analysis employed in the current research has examined the relationships in the model and offers key insights about the relationships between the constructs in the model. To further investigate the relationships between the constructs, all relationships in the model could be examined simultaneously in subsequent studies by utilizing CB-SEM (e.g AMOS or LISREL), SPSS or other appropriate techniques.

References

Aldridge, A., White, M., & Forcht, K. (1997), "Security considerations of doing business via the internet: cautions to be considered," Internet Research: Electronic Networking Applications and Policy, 7(1), 9-15.

Anderson, J.C., & Gerbing, D.W. (1988)," Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," Psychological Bulletin, 103 (3), 411–423.

Bhattacherjee, A. (2001)," Understanding information systems continuance: An expectation-confirmation model," MIS Quarterly, 25(3), 351-370.

Bhattacherjee, A. (2002)," Individual trust in online firms: scale development and initial test," Journal of Management Information Systems, 19(1), 211-242.

Bhimani, A. (1996),"Securing the commercial Internet," Communications of the ACM, 39(6), 29-35.

Chin, W.W. (1998), "The Partial Least Squares Approach to Structural Equation Modeling", in G.A. Marcoulides [ed.]. Modern Methods for Business Research, pp. 295-336. Mahwah, NJ: Lawrence Erlbaum Associates, Publisher.

CIMB Bank, (2001), "Security Policy", http://www.cimbclicks.com.my/security-policy.html

Chin, W.W. (2010),"How to write up and report PLS analyses," In V. Esposito Vinzi, W.W. Chin, J. Henseler, & H. Wang (Eds.), Handbook of partial least squares: Concepts, methods and application (pp. 691-711). New

York: Springer. Doi:10.1007/978-3-540-32827-8_29

Chung, B., & Skibniewski, M. (2007)," An implementation strategy for integrated enterprise systems in construction," Paper presented at the ASCE/CIB Construction Research Congress, Newport, Bahamas.

Culnan, M.J., & Armstrong, P.K. (1999)," Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," Organization Science, 10(1), 104-115.

Huang, D-L., Rau, P-L. P., & Salvendy, G. (2007)," A survey of factors influencing people's perception of information security," In J. Jacko (Ed.): *Human-Computer Interaction. HCI Applications and Services* (pp. 906-915). Springer Berlin Heidelberg. DOI: 10.1007/978-3-540-73111-5_100

Featherman, Mauricio S., & Pavlou, Paul A. (2003). Predicting e-services adoption : A perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*, 451-474.

Flavia´n, C. and Guinalı´u, M. (2006)," Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site," Industrial Management & Data Systems, 106(5), 601-620.

Fornell, C. and Bookstein, F.L. (1982),"Two structural equation models: LISREL and PLS applied to consumer exit-voice theory, "Journal of Marketing Research, 19 (4), Special Issue on Causal Modeling, 440-452.

Fornell, C., & Cha, J. (1994)," Partial least squares. In R. P. Bagozzi (Ed.), Advanced Methods of Marketing Research (pp. 52-78)," Cambridge, MA: Blackwell.

Fornell, C., & Larcker, D. F. (1981)," Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, 18(1), 39 – 50.

Furnell, S.M., & Karweni, T. (1999)," Security implications of electronic commerce: a survey of consumers and businesses," Internet Research: Electronic Networking Applications and Policy, 9(5), 372-382.

Gefen, D. (2000),"E-commerce: the role of familiarity and trust," Omega, 28(6), 725-737.

Gholami, R., Sulaiman, A. B., Ramayah, T., & Molla, A. (2013),"Senior managers' perception on green information systems (IS) adoption and environmental performance: Results from a field survey," Information and Management, 50(7), 431-438.

Goodwin, C. (1991), "Privacy: Recognition of a consumer right," Journal of Public Policy Marketing, 10(1) (Spring 1991), 106-119.

Mohan, H., Ahmad, N., Quah, C.k., Chiam, t.y., Liew, j., & Nik mat, n.k., (2013)," Determinants of the Internet Banking Intention in Malaysia," American Journal of Economics, 3(3), 149-152. Doi: 10.5923/j.economics.20130303.03

Hoffman, D.L., & Novak, T. P. (1997)," A new marketing paradigm for electronic commerce," Information Society: An International Journal, 13(1), 43-54.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999),"Building consumer trust online," *Communications of the ACM, 42*(4), 80-85.

Hussin, A. R. C., Dahlan, H. M., & Bahari, M. (2009), "A consumer perception trust model for e-commerce", FRGS Grant Report, Universiti Teknologi Malaysia, http://eprints.utm.my/9788/1/78196.pdf

Jano, z., janor, h., elangsegaran, r., khamis, n., md saad, m.s., (2012)," Internet banking: Analysing encouragement and impediment factors among academicians," International Journal of Computer Networks and Wireless Communications (IJCNWC), 2(3), 335-341.

Kim, D.J., Steinfield, C., & Lai, Y. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44*(4), 1000-1015.

Lewieki, R.J., & Bunker, B. B. (1995)," Trust in relationships: a model of trust development and decline," In Bunker, B.B. (Ed): Rubin, J.Z. (Ed), (1995). Conflict, cooperation, and justice: Essays inspired by the work of Morton Deutsch. The Jossey-Bass management series and The Jossey-Bass conflict resolution series, (pp. 133-173). San Fransisco, CA, US: Jossey-Bass.

Mayer, R.C., Davis, J.H., & Schoorman, F.D. (1995)," An integrative model of organizational trust," Academy of Management Review, 20(3), 709-734.

Mukherjee, A. and Nath, P. (2007),"Role of electronic trust in online retailing: a re-examination of the commitment-trust theory," European Journal of Marketing, 41(9/10), 1173-1202

Raman, m., Stephenaus, r., alam, n., & kuppusamy, m., (2008)," Information Technology in Malaysia: E-service quality and Update of Internet banking," Journal of Internet Banking and Commerce, 13(2), 1-18.

Ndubisi, N.O., & Sinti, Q. (2006)," Consumer attitudes, system's characteristics and internet banking adoption in Malaysia," Management Research News, 29(1/2), 16-27.

Normalini, M. K. And Ramayah, T. (2013), "Understanding Security in Consumer Adoption of Internet Banking: Biometrics Technology Implementation in the Malaysian Banking Context," Handbook of Research and Development in E-Business through Service-Oriented Solutions, Editor: Katalin Tarnay, Sandor Imre & Lai Xu, IDEA Group International (IGI Global), Chapter 15, 293-306. ISBN: 9781466641815

Mozie, N.m., Mustapha, r.m.r., & ghazali, n. (2012)," Perceived Trustworthiness and the Behavioral Intention to Use Internet Banking Service among Bank Users in Shah Alam, Selangor," Paper presented at the International Conference on Innovation, Management and Technology Research (ICIMTR2012), Malacca, Malaysia, May 2012 (pp.23-27), IEEE

Poon, W.C. (2007),"Users' adoption of e-banking services: the Malaysian perspective," Journal of Business & Industrial Marketing, 23(1), 59-69.

Ramayah, T., Wai, j.c.l., & Boey, J. C. I. (2011), "Network collaboration and performance in the tourism sector," Service Business, 5(4), 411-428.

Ratnasingham, P. (1998), "The importance of trust in electronic commerce," Internet Research: Electronic Networking Applications and Policy, 8(4), 313-321.

Ringle, C.M., Wende, S. & Becker, J. M. (2014),"Smartpls 3," Hamburg: SmartPLS," Retrieved from http://www.smartpls.com

Roca, J.C., Garcia, J.J., & de la Vega, J.J. (2009)," The importance of perceived trust, security and privacy in online trading systems," Information Management & Computer Security, 17 (2), 96-113.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (1998),"Not so different after all a cross-discipline view of trust," Academy of Management Review, 23(3), 393-404.

Sang, S., Lee, J. D., & Lee, J. (2010)," E-government adoption in Cambodia: A partial least squares approach," Transforming Government: People, Process and Policy, 4(2), 138-157.

Sathye, M. (1999)," Adoption of Internet banking by Australian consumers: an empirical investigation," International Journal of Bank Marketing, 17(7), 324-334.

Suganthi, r., Balachandher, k.g. & Balachandran, S. (2001)," Internet banking patronage: an empirical investigation of Malaysia," Journal of Internet Banking and Commerce, 6(1). www.arraydev.com/commerce/JIBC/0103_01.htm

Suh, B., & Han, I. (2003),"The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," International Journal of Electronic Commerce, 7(3), 135-161.

Yousafzai, S. y., Pallister, J. G., & Foxall, G.R. (2003),"A proposed model of e-trust for electronic banking," Technovation, 23(11), 847-860.

Yousafzai, S., Pallister, J., & Foxall, G. (2009),"Multi-Dimensional Role of Trust in Internet Banking Adoption," The Service Industries Journal, 29(5), 591-605.

Yu, W. W. (2002), "Maybank targets consumers," News Straits Times (Malaysia), April 3, 2002, Edition 2, News and Analysis Section.