Journal of Management Sciences
Vol. 4(1): 3-26, 2017
DOI: 10.20547/jms.2014.1704101

Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security

Normalini M.K [*] T. Ramayah [†]

Abstract: *Internet banking is gaining popularity in Malaysia due to its convenience which is achieved by unique business interactions between banking institutions and customers via websites and mobile applications. However, the incredible escalation of internet fraud cases has caused increased privacy and security risks for internet banking customers. Based on a review of literature, this paper developed a research framework to gauge the impact of customer perception about the effectiveness of biometrics technology on perceived privacy and security and its influence on trust and intention to continue internet banking. In light of the growing viability of biometrics technology as a solution for internet banking issues, the developed framework is then used to assess whether perceptions of biometrics effectiveness for internet banking has significant impact on the relationship between trust and perceptions of privacy as well as security. By testing the framework using a sample of 413 internet banking users, this study offers significant insights into the potential effectiveness of biometrics technology application in an internet banking context to alleviate privacy and security concerns and improve trust among Malaysian customers. The findings revealed that although there was an insignificant relationship between perceived privacy and trust, perceived biometrics effectiveness significantly influenced the strength of the relationships between both perceived privacy and perceived security with trust.*

Keywords: Internet banking, Effectiveness of biometrics, Privacy, Security, Trust, Intention to continue.

Introduction

In today's high speed world, those involved in the millions of financial transactions occurring every minute need to be assured that data is readily available but also kept secure at all times. Among the many institutions in the financial landscape, the banking sector especially has been changing due to technological advancements. Society has drastically altered the way they perform banking activities due to the development of internet banking. Lichtenstein and Williamson (2006) found that the implementation of Internet banking by banks could deliver reduced costs of operations, improved quality of services, and a positive stream of customers.

[*]PhD, School of Management, Universiti Sains Malaysia.
E-mail:normalini_mk@yahoo.com
[†]Professor, School of Management, Universiti Sains Malaysia.

Presently, the central bank of Malaysia, Bank Negara Malaysia, has licensed twenty seven commercial banks consisting of eight Malaysian banks and nineteen foreign banks (*Commercial Banks*, 27 January, 2015). Besides that, there are also sixteen Islamic banks, four international Islamic banks, twelve investment banks and two other financial institutions (*Commercial Banks*, 27 January, 2015). With the rise of Internet banking and registered banking institutions in Malaysia, there are now 31 banking institutions offering Internet banking services while 13 institutions offer mobile banking services (*Commercial Banks*, 27 January, 2015).

The increase in the number of institutions offering such services has resulted in the staggering growth of Internet banking subscribers in the country. By the year 2014, the total number of internet banking subscribers rose to 17.6 million or 58.2% of the population a significant leap from 2.6 million or 9.8% of the population in 2005 (*Payment Statistics*, 2013). From 25, 000 subscribers in 2002 (W. Yu, 2002), Maybank (one of the pioneers of Internet banking in Malaysia) via its Maybank2u application, now has over 7.8 million registered users who access the banking portal via personal computers and mobile devices (*The Star Online Business*, 2015).

Unfortunately, the rising numbers of internet banking users have attracted the attention of unscrupulous high-tech savvy criminals who use innovative ways to steal information and funds from individuals and companies around the world. MyCERT (Malaysian Computer Emergency Response Team) Security Breaches statistics shows an increasing trend of reports received every year from the year 2005 to 2011 (58 reports to 15218 reports or a 26,137.93% increase), with a drop in 2012 followed by a steady rise again from 2012 to 2014 (9986 reports to 11918 reports or a 19.35% increase) (*MyCERT*, 2014).

In 2014, the majority of reports were due to fraud and spam, followed by intrusion attempts and intrusion (*MyCERT*, 2014). Fraud incidents were mostly due to phishing sites of local and foreign institutions. Incidents related to system intrusions were generally caused by web defacement in vulnerable web applications. The sheer numbers of increasing reports are a cause for concern, especially for those conducting internet banking. Once attacked, there is a high probability that online banking customers would experience an irrecoverable loss of personal information and savings. The Malaysian country manager of Sourcefire Incorporated, a networking security and intrusion prevention company, stated that security incidents, privacy breaches and business disruption in Malaysia have resulted in estimated losses of more than RM3 billion over a period of five years before 2013 (Kumar, 2013).

Biometrics technology is emerging as a potential solution for privacy and security issues in internet banking. Overview of the existing biometric technologies along with their composition, classification and performance evaluation indicators have been discuss by (Unar, Seng, & Abbasi, 2014). Despite its promise, biometrics authentication technology has yet to gain wide acceptance among banks and consumers. As such, the framework developed in this study is timely as it has the potential to provide crucial data pertaining to the perception of the effectiveness of biometrics technology usage in Internet banking systems. Insights gained from the empirical study conducted based on this framework should assist Internet banking providers in formulating new policies and measures that improve handling of privacy and security issues related to Internet banking. More efficient, reliable and

secure online banking services will then foster economic growth and lead Malaysia further towards its goal of becoming a developed country.

Literature Review

In light of the growing importance of Internet banking and corresponding privacy and security concerns, there have been an increasing number of studies focusing on this area. Shortly after the introduction of Internet banking in Malaysia in the year 2000, the rate of expansion and adoption of Internet banking was comparatively low (Suganthi, 2001). Even though the electronic transformation had begun in Malaysia, the banking industry could not advance acceptance of Internet banking successfully (Ndubisi, Sinti, & Chew, 2004). The study that done by (Ben Mansour & Ben Mansour, 2016) stated that by considering the important amounts that have been invested in Internet banking systems throughout the world, it is of paramount importance to ensure that business users will actually use them. Somehow Internet banking professionals need to develop the beliefs of usefulness, ease of use, credibility and integrity of business users regarding Internet banking.

While various factors have been found to have an impact on adoption levels and the intention to use Internet banking, trust has been found to be a key factor in Internet banking development (S. Yousafzai, Pallister, & Foxall, 2009). As important as trust is in conventional banking, it is even more crucial in Internet banking due to higher levels of uncertainties present in an online setting (Ratnasingham, 1998; Akhlaq & Ahmed, 2013). Unsurprisingly, (Hoffman, Novak, & Peralta, 1999) found that the willingness of users to exchange money and sensitive personal information online was highly influenced by trust. Zhu (2015) concluded that without sufficient trust, Internet banking services would be unsuccessful.

Nasri and Charfeddine (2012), citing (Bestavros, 2000; Furnell & Karweni, 1999), stated that developing customer trust over privacy and security issues is the ultimate challenge facing e-banking institutions. Lallmahamood (2007) found that the main reasons non-Internet banking customers did not use online services were due to trust, security, and privacy concerns. When customers are not assured that their personal information is protected, there is a perception that the banking system does not have a high level of security; the customer's trust in the banking institution will then be affected and this in turn will negatively affect the customer's intention to engage in online banking (S. Y. Yousafzai, Pallister, & Foxall, 2003).

Many studies have identified privacy and security as the main reasons for customer distrust in Internet banking as lack of trust is not only the result of deficiencies in Internet and system security but also privacy concerns (Suh & Han, 2003; White & Nteli, 2004). Privacy relates to mechanisms for personal information protection while security relates to protection mechanisms for all types of data as well as assets. Even in new innovations like cloud computing, which has recently been implemented in Internet banking (Apostu, Rednic, & Puican, 2012), security and privacy remain among the most important factors affecting trust (Uusitalo, Karppinen, Juhola, & Savola, 2010).

Existing literature has also found that privacy and security factors are among the most

important factors related to Internet banking technology adoption. Sathye (1999) reported that privacy and security were found to be significant obstacles to the adoption of online banking in Australia. (Ramayah & Ling, 2002) and (Poon, 2007) discovered that the reluctance to adopt and apply Internet banking in Malaysia was due to concerns about privacy and security issues. However, adoption of Internet banking has greatly increased as can be seen by the rising numbers of Internet banking subscribers in Malaysia.

Even so, privacy and security factors have remained important as a significant number of banking institutions face cyber attacks amounting to tens of thousands attacks either weekly or monthly (Kumar, 2013). As there are constantly increasing number of ways to penetrate privacy and security mechanisms, the risk of information theft, transaction tampering and corruption of data could become a reality for many. If security breaches occur, customers may incur damages ranging from privacy invasion to financial loss (Suh & Han, 2003). These fears have been captured by a recent study by (Amin & Ramayah, 2010) who found that SMS banking adoption in Malaysia was significantly influenced by security and privacy concerns.

The targeted and sophisticated tactics used across Asia has made it clear that privacy and security challenges have to be approached in new ways (Kumar, 2013). Thus, Internet banking requires the advancement of technology to enable more secure, efficient and convenient services for customers. Investment in innovative technologies has to occur in order to prevent lasting damage to business and reputation. Biometrics technology offers banking institutions a number of benefits to counter these challenges.

Biometric technology has been named as one of the top ten technologies that will change the world (Cameron, 2016). It provides a range of automated methods which can be used to measure and analyze a person's physiological and behavioural characteristics (Alhussain & Drew, 2009). According to (Lupu & Lupu, 2015a), stated that security in internet banking applications can be improved by using biometrics for the authentication process. Several biometric traits have been proven useful for biometric recognition (Faundez-Zanuy, 2006). Currently, commonly used biometric include fingerprint, iris, face, and voice recognition technology that is applicable to a wide variety of fields including use in government buildings, airports, banks, and others. Anticipated decrease in technology costs, improved technical quality of the systems and socio-political pressures for better security-related controls has generated increased interest in biometrics technology (Pons & Polak, 2008).

Biometric identification systems can significantly reduce or mitigate risks related to security and personal information fraud compared to traditional identification means (Miltgen, Popovič, & Oliveira, 2013). Government agencies in particular have started to use biometrics to minimise internal and external threats and consequently improve public safety. Studies have examined the intention of using biometrics technology (Seyal & Turner, 2013) as well as its implementation (Alhussain & Drew, 2009) in the government sector. However, there has not been much research done on biometric systems from a consumer acceptance perspective (Miltgen et al., 2013; Morosan, 2010).

Furthermore, implementation of biometrics technology in Internet banking is still a relatively new idea and there is little empirical research conducted to assess the acceptance of this technology amongst banking customers. One study conducted in India shows that biometric authentication can be superior to and is preferred over traditional authentica-

tion systems such as the use of personal identification numbers (Chopra & Sherry, 2014). Nevertheless, underutilization of biometrics technology is possible when users feel fearful, hesitant, or uncomfortable with the technology (Scott, Acton, & Hughes, 2004).

Consequently, it is important to investigate the perceptions of users as resistance can lead to an increased risk of biometrics implementation failure (Pons & Polak, 2008) and thus reduce trust in an institution. Furthermore, as a variety of reasons can influence the acceptance of biometrics technology, it is crucial to study how biometrics technology is affected by different factors (Pons & Polak, 2008; Morosan, 2010) as well as affects factors that lead to greater intention to use internet banking. As privacy and security are important factors in internet banking, studying how the effectiveness of biometrics technology affects the relationship between these factors and trust would enable banks to make important enhancements to meet specific customer needs as well as facilitate expansion to draw in new customers.

Therefore, the main objective of this research is to understand these issues from the perspective of the Malaysian Internet banking user. Furthermore, not many studies have linked privacy and security issues in Internet banking to biometrics technology. Hence, the framework is designed to facilitate the examination of the moderating influence of perceived biometrics technology effectiveness on the relationship between perceived privacy and perceived security to trust. The findings of this study will be useful for banking institutions in Malaysia to determine the type of biometrics system and features required to positively influence customer intention to use internet banking.

Research Framework and Hypotheses

Pavlou and Fygenson (2006) found that numerous studies in the field of e-commerce have used the Technology Acceptance Model (TAM) (Davis, 1989), as well as the models that it is based on (Theory of Reasoned Action (Fishbein & Ajzen, 1977) and Theory of Planned Behavior (Ajzen, 1991)), to show that the involvement of customers in e-commerce can be significantly predicted by their intentions to engage in online transactions.

This study has extended the TAM model (which is an information systems theory that predicts how users respond to new technology) to enable researchers to further understand the important factors that specifically influence intention to continue using Internet banking applications. Trusting beliefs are partly formed outside the online environment itself just as beliefs and attitudes are formed (Salo & Karjaluoto, 2007). Although in the original TAM model attitude is a predictor of intention, trust can be seen as a better predictor of intention. This is because without trust in banking institutions, customers would not intend to use internet banking. As the Internet is an open transaction infrastructure that stretches worldwide, trust has become a crucial element of e-commerce (Hoffman et al., 1999) and related applications like Internet banking.

Additionally, using an extended TAM model to understand how biometrics technology can affect trust and intention to continue using Internet banking is crucial as designs of systems that use digital identities (such as biometrics technology) require the consideration of end user perception and behavioural response (Jones, Antón, & Earp, 2007). Customers'

technological orientation and perception of the technological competency of an electronic system is very important in their information processing behaviour and perceived trust towards electronic banking (S. Y. Yousafzai et al., 2003).

Moreover, the original constructs of the model, perceived ease of use and perceived usefulness, have been replaced by perceived privacy and security as these issues are often a major source of concern to consumers (Deane, Barrelle, Henderson, & Mahar, 1995; Adam, Dogramaci, Gangopadhyay, & Yesha, 1998), especially internet banking customers. Furthermore, (Rajaobelina, Ricard, Bergeron, & Toufaily, 2014) found that many researchers (Rajaobelina et al., 2014) have recognised that both security and privacy are important antecedents of online trust. Salisbury, Pearson, Pearson, and Miller (2001) found that most research related to perceived security is rooted in TAM as external variables (such as perceived privacy and security) influence how and when users will use new technology.

Although perceived privacy and security variables in internet relationships have particular characteristics that establish them as distinct concepts; consumers, companies and legislators perceive that they are closely related (Flavián & Guinalíu, 2006). Besides, (Adam et al., 1998) stated that ensuring security and privacy are fundamental prerequisites for all commercial activities involving sensitive information. Moreover, (Hoffman et al., 1999) found that security and privacy concerns determine the extent to which customers can trust and feel comfortable proceeding with online transactions.

Considering these factors, the main question underlying the development of the framework is: What are internet banking users' perceptions towards the effectiveness of usage of biometrics authentication technologies in online banking systems? The secondary questions are as follows: a) Does perceived privacy affect customers' trust in Internet banking? b) Does perceived security influence customers' trust in Internet banking? c) Does trust in Internet banking influence the intention to continue using Internet banking? and d) Does perceived effectiveness of usage of biometrics authentication technologies moderate the relationship between perceived privacy and security to trust in Internet banking?

Five hypotheses are proposed in this framework based on prior research and the proposed research questions. Each hypothesis is stated in the sections below as H1, H2, H3, H4 and H5. The framework (see Figure 1) depicts how trust influences intention to continue using internet banking by exploring the relationship between perceived privacy and security to trust and the moderating role of perceived effectiveness of usage of biometrics technology.

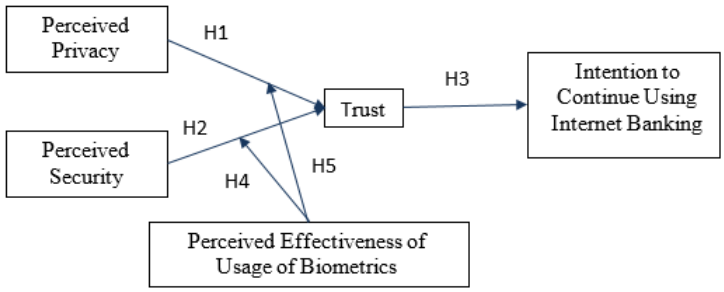
Perceived Privacy

S. Y. Yousafzai et al. (2003) defined perceived privacy as the "customer's perception regarding their ability to monitor and control information about themselves." It is the guarantee that personal information about customers collected from their electronic transactions is protected from disclosure without permission. Hoffman et al. (1999) revealed that lack of trust arises from cyber-consumers' perceived lack of control over the access others have of their personal information during the online navigation process. Loss of privacy leads to loss of confidentiality, a significant factor in building trust (Culnan & Armstrong, 1999). Thus, privacy is an important part of building trust and a long-term relationship between

users and institutions operating online sites (Ma, 2012). As such, this study proposed that:

- *H_1: Perceived privacy has a positive impact on the customer's trust in Internet banking.*

Figure 1
Research Framework



Perceived Security

Perceived security is defined as the "customer's perception of the level of protection against security threats" (S. Y. Yousafzai et al., 2003). Basic security principles that are crucial for e-commerce have been highlighted by a number of researchers (Ratnasingham, 1998; Furnell & Karweni, 1999; Suh & Han, 2003; Gefen, 2000).

As banks are seeking greater market expansion, Internet banking diffusion is important but is affected by rising identity fraud and online scams which are resulting in increased security concerns. The Asia Pacific region's malware infection rates and botnet drones are above the worldwide average (Kumar, 2013). In addition, Malaysia has been known to have the world's highest concentration of phishing sites (Kumar, 2013). Other cyber crime attacks on financial institutions in the region have been attributed to Trojans (Kumar, 2013). In addition, there are now fake mobile banking applications that compromise banking information stored on the device in order to facilitate bank/credit card fraud (Kumar, 2013). Furthermore, the TrendLabs first quarter 2014 Security Roundup report by security solutions provider Trend Micro Inc. showed that Malaysia was among the top ten countries afflicted by online banking malware (*Malay Mail Online*, 2015). Worse, there have been many new techniques explored by those who create banking malware that steer away from the traditional delivery mechanism of ZIP and RAR files to utilize newer malicious .CPL files (Control Panel files for Microsoft Windows) embedded in .RTF (Rich Text Format) documents (*Malay Mail Online*, 2015).

Security alerts have been issued by many banks in the Asia Pacific region concerning relentless malware such as newer Zeus variants and Spyeye (Kumar, 2013). *MyCERT* (2014) recently received several reports regarding the Zeus banking malware family which

injects modified fake contents or pages while a user is browsing a legitimate online banking website. The attackers will then login to the victim's online banking account using the stolen credentials and perform online transactions successfully using intercepted TAC numbers (*MyCERT*, 2014).

The way banks deal with erroneous transactions and security concerns that may occur during online banking will influence customer confidence in e-banking (Sohail & Shanmugham, 2003). Ndubisi et al. (2004) found that raising public confidence for system utilization involved the important aspect of security adequacy. This is in line with studies on Malaysian consumers which found that the lack of security and unreliability of transactions over the Internet affect Internet banking adoption (Lu, Hsu, & Hsu, 2005; Sudha, Thiagarajan, & Seetharaman, 2007; Anuar, Adam, & Mohamad, 2012).

Further studies on Internet banking in Malaysia have found that adoption levels were influenced by security and trust (Pons & Polak, 2008; Md Nor & Pearson, 2007; Amin, 2007; YenYuen & Yeow, 2008). Kim, Steinfield, and Lai (2008) found that consumer's trust towards an institution is increased by perceptions of security protection which also decreases the perceived risk in completing the transaction. Feelings of security increase the customer's willingness to trust (Salo & Karjaluoto, 2007) as they feel that the institution is more reliable and are consequently more comfortable to perform transactions.

Therefore, security as well as privacy has been identified as key antecedents of trust which in turn positively influences the behavioural intention of customers (Arnott, Wilson, Mukherjee, & Nath, 2007). Hartono, Holsapple, Kim, Na, and Simpson (2014) found that although security was conceptualised as a multidimensional construct, this was inconsistent with the way empirical studies operationalised measures of perceived security. Hence, the multidimensionality of perceived security is ignored and instead most researchers study perceived security as one dimension. For that reason, this research posited that:

- *H_2: Perceived security has a positive impact on the customer's trust in Internet banking.*

Trust and Intention to Use Internet Banking

Trusting belief refers to the belief that one can rely upon a promise made by another and that the other, in unforeseen circumstances, will act toward oneself with goodwill and in a benign fashion (Grazioli & Jarvenpaa, 2000). This is similar to customer trust in internet banking, which is defined as the "psychological state which leads to the willingness of customers to perform banking transactions on the Internet, expecting that the bank will fulfill its obligations, irrespective of customer's ability to monitor or control ban's actions" (Mayer, Davis, & Schoorman, 1995; Rousseau, Sitkin, Burt, & Camerer, 1998).

Although trust has been research widely in the information technology field, it is still not a prominently researched concept in internet banking. Trust is of supreme importance in internet banking due to the lack of physical presence and interaction between banks and customers. Trust is especially important because of the apparent physical distance between transacting parties which leads to increased risks (Gefen & Straub, 2003), such as privacy and security risks. Researchers have studied the impact of trust on internet

banking use and found that trust significantly influences the customer's intention to use internet banking (Suh & Han, 2003; Sohail & Shanmugham, 2003; Bhattacherjee, 2002; Md Nor & Pearson, 2007).

Trust is seen as one of the main obstacles that hinder individuals from adopting internet banking technology (Md Nor & Pearson, 2007). Akhlaq and Ahmed (2013) found that lack of trust negatively affects intention to use internet banking. As online transactions involve sensitive information and valuable fund transferred via the Internet (Suh & Han, 2003), trust would favourably be influenced with increased perceptions of privacy and security among internet banking customer, thereby leading to greater intention to use internet banking. Considering the results of previous studies, this study strongly suggested that:

- *H_3: Trust has a positive impact on customer's behavioural intention to continue using Internet banking services.*

Effectiveness of Usage of Biometrics Technologies

Although security and privacy are viewed as important service dimensions of internet banking, solutions to enhance privacy and security using conventional methods do not seem to be effective. Customer concerns about the trustworthiness of internet banking systems in handling information and managing funds affect their intention to use the system (Lee, Kwon, & Schumann, 2005). According to (Uzoka & Ndzinge, 2009), there are three basic approaches for the verification of an individual's identity: something the person has (e.g., Debit card), something the person knows (e.g., password, PIN) and something the person is (e.g., fingerprint), which is unique about the person and cannot be shared.

Credit cards, username and passwords that have been used for authentication by many institutions are no longer sufficient to guarantee the privacy and security banking customers. Stronger consumer authentication in online environments is necessary to protect and preserve customer safety, confidence, and acceptance (Williamson & Money-America's, 2006). Biometric technology is emerging as the latest solution to tackle privacy and security concerns in Internet banking (Fatima, 2015). It is easier and safer to login to Internet banking with something you have or are (fingerprint, face, iris etc.) than with something you remember. Biometrics can be used on desktop/laptop computers, but also on smart phones, many of them being equipped with a fingerprint sensor (Lupu & Lupu, 2015b). Biometrics provides a range of automated methods for identification and verification which can be used to measure and analyze behavioural (speech recognition, signature and keystrokes) and physiological (fingerprint, facial recognition, iris scan, retinal scan, vascular patterns and hand geometry) characteristics (Alhussain & Drew, 2009; Seyal & Turner, 2013). The benefits related to the implementation of biometric technologies in online applications are supported by many researchers (Alhussain & Drew, 2009; Uzoka & Ndzinge, 2009; Harby, Qahwajim, & Kamala, 2010). As privacy and security issues can be improved by using biometrics technologies, the biometrics industry has been growing steadily in developed countries like US and Japan.

Some researchers have studied the implementation of biometrics technology in banks including (Alhussain & Drew, 2009), who examined how facial recognition systems at

ATMs were able to reduce potential theft. The benefits of biometric authentication tools in online banking systems include securing the log-in process to systems, removing password vulnerabilities, enhancing convenience, reducing data vulnerability and help desk costs by eliminating password reset requests (Harby et al., 2010). According to (Pranić, Roehl, & West, 2009), it is imperative to make a distinction between biometrics acceptance and perceived effectiveness as it is important to understand biometrics implementation from the consumer point of view as well as the technology point of view (Pranić et al., 2009).

In Malaysia, biometrics technologies have been implemented in the government sector. The National Registration Department, the largest user of biometrics technology in Malaysia, use national identity cards to keep biometrics data through embedded microchips. The immigration department has also implemented an auto-gate system at various entry points in the country, utilizing thumb print authentication systems to match scanned thumb prints with biometric data in microchips embedded in passports. Banking institutions also require thumb print authentication for every high risk transaction in physical bank branches.

However, application of biometrics technology in online banking is still at an early stage. A study by (Saripan & Hamin, 2011) found that behavioral authentication in the form of digital signature authentication technology provided by internet banking institutions has been underutilized by individual internet banking customers in Malaysia as compared to corporate customers due to technological and legal weaknesses.

Biometrics can potentially become a key driver of growth for Malaysia if the country is able to lead in biometrics technology advancements to fulfil global and national needs. As the Malaysian government has always emphasized privacy and security protection in financial, economic, and political activities, biometrics technology could lead to the achievement of this goal. Therefore, it was hypothesised that:

- *H_4: The higher the perceived security the higher the customer's trust in Internet banking if perceived effectiveness of usage of biometrics technologies is high.*

- *H_5: The higher the perceived privacy the higher the customer's trust in Internet banking if perceived effectiveness of usage of biometrics technologies is high.*

Research Method

The framework was tested through the use of a survey questionnaire. Items used in the questionnaire were adapted from several different sources to reduce method bias. In addition to the items measuring the variables in the framework, several items to collect information about respondents was included in the questionnaire. The sources of measures for all variables are found in Table 1.

Table 1
Source of Questionnaire Items

Frequency	Percentile
Perceived Privacy	Featherman & Pavlou (2003)
Perceived Security	Yousafzai et al. (2009); Suh & Han (2003)
Trust	Suh & Han (2003); Yousa fzai et al. (2009)
Intention to Continue Using	Bhattacherjee (2001); Chung & Skibniewski (2007)

Self-administered questionnaires were distributed using the drop-off and pick-up (DOPU) method to bank branch managers who were willing to distribute the questionnaires to their customers. Respondents were confined to a specific population (internet banking users in Peninsular Malaysia using local or foreign internet banking services) in line with the purposive sampling method (Sekaran, 2006). A total of 452 questionnaires were collected but only 413 questionnaires were completed. Data was analyzed using statistical methods as found in the section below.

Results

The model developed for this research was tested with the structural equation modelling (SEM) technique using partial least squares (PLS) by means of the SmartPLS 3.0 software (Ringle, Wende, & Becker, 2015). SmartPLS is a second generation statistical analysis software that can be used to test complex models with latent variables. The two-stage analytical procedure recommended by (Anderson & Gerbing, 1988) was conducted. First, the measurement model was tested to validate the instrument. Second, structural model testing was done to test the hypothesized relationships.

Measurement Model Analysis

To assess measurement models, literature suggests that researchers look at indicator loadings, average variance extracted and also composite reliability values which measure convergent validity. Convergent validity evaluates whether or not items that represent a construct reflect the same construct in reality. The loadings of the indicators were first assessed to determine whether they were above the threshold of 0.6 (Chin, Gopal, & Salisbury, 1997; Gholami, Sulaiman, Ramayah, & Molla, 2013; Raza & Hanif, 2013; Raza, Qazi, & Umer, 2016). Values for average variance extracted (AVE) had to be above 0.5 and composite reliability (CR) values above 0.7 (Hair, Black, Babin, & Anderson, 2010). As can be seen from Table 2, all relevant values were above the recommended threshold thus convergent validity was achieved.

Many prior studies have used the (Fornell & Larcker, 1981) criterion to test for discriminant validity. There has been recent criticism that the (Fornell & Larcker, 1981) criterion does not reliably detect the lack of discriminant validity in common research situations (Henseler, Ringle, & Sarstedt, 2015). An alternative approach has been suggested based on the multi trait-multi method matrix to assess discriminant validity. The approach, heterogeneity-mono trait (HTMT) ratio of correlations, has been demonstrated by (Henseler et al., 2015) through a Monte Carlo simulation study to have superior results.

Table 2
Measurement Model

Construct	Item	Loadings	AVE	CR
Intention	INT1	0.944	0.860	0.961
	INT2	0.897		
	INT3	0.942		
	INT4	0.925		
Perceived Biometrics Effectiveness	PEOUBT1	0.944	0.690	0.939
	PEOUBT2	0.865		
	PEOUBT3	0.906		
	PEOUBT4	0.904		
	PEOUBT5	0.722		
	PEOUBT6	0.845		
	PEOUBT7	0.681		
Perceived Privacy	PP1	0.680	0.726	0.837
	PP3	0.995		
Perceived Security	PS1	0.881	0.837	0.962
	PS2	0.923		
	PS3	0.938		
	PS4	0.927		
	PS5	0.904		
Trust	TRUST1	0.921	0.869	0.964
	TRUST2	0.942		
	TRUST4	0.950		
	TRUST5	0.915		

Note: PP2 and Trust 3 was deleted due to low loadings

As such, the discriminant validity values of this study have been calculated using this new method and the results are shown in Table 3. A problem of discriminant validity is found when the HTMT value is greater than $HTMT_{0.85}$ (HTMT value of 0.85) (Kline, 2015), or $HTMT_{0.90}$ (HTMT value of 0.90) (Gold & Arvind Malhotra, 2001). As shown in Table 3, all values passed both the $HTMT_{0.90}$ (Gold & Arvind Malhotra, 2001) and $HTMT_{0.90}$ (Kline, 2015) thresholds, indicating that discriminant validity was achieved.

Table 3
Heterotrait-Monotrait Ratio (HTMT) of correlations test for Discriminant Validity

Construct	1	2	3	4	5
Intention					
Perceived Biometrics Effectiveness	0.554				
Perceived Privacy	0.038	0.080			
Perceived Security	0.577	0.586	0.049		
Trust	0.801	0.589	0.023	0.622	

Structural Model Analysis

Table 4 presents the results of the hypotheses testing. The structural model testing showed that Perceived Security was positively related ($\beta = 0.383$, $p < 0.01$) to Trust while Perceived Privacy was not significantly ($\beta = -0.032$, $p > 0.05$) related explaining 42.9% of the variance. Trust was also positively related ($\beta = 0.760$, $p < 0.01$) to Intention to Use explaining 57.8% of the variance. Thus, H2 and H3 were supported while H1 was not supported. The predictive relevance (Q2) values were higher than 0 as suggested by (Fornell & Cha, 1994) with Trust having a Q2 value of 0.391 and Intention to Use with a Q2 value of 0.496. The f2 values were all greater than 0.02 indicating that there was substantive significance on top of statistical significance. Further investigation was conducted to assess whether multicollinearity would be an issue however all VIF values were found to be less than 5 as suggested by (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014).

To assess whether perceived effectiveness of biometrics technologies usage moderated the relationship between perceived security and trust as well as perceived privacy and trust, the product indicator approach was used by adding the interaction terms to the equation. Both the interaction terms were significant [Perceived Security * Biometrics Effectiveness ($\beta = 0.074$, $p < 0.01$); Perceived Privacy * Biometrics Effectiveness ($\beta = 0.077$, $p < 0.01$)] adding 3% of variance. Thus, H4 and H5 of this study were also supported.

Table 4
Hypotheses Testing

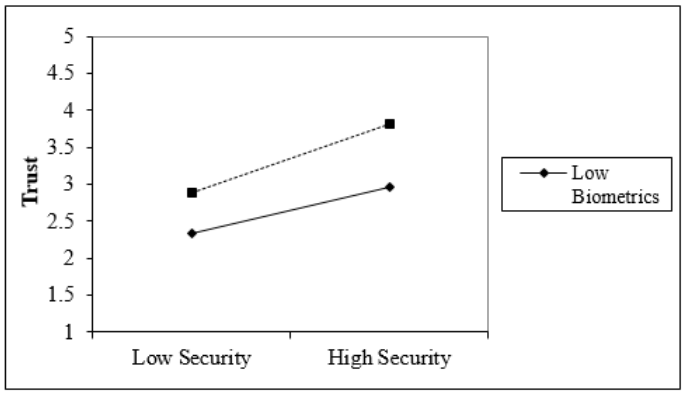
Hypothesis		Std. Beta	Std. Error	t-value	Decision	f^2	Q^2	R^2	VIF
H1	Perceived Privacy → Trust	-0.032	0.035	-0.922	Not Supported	0.002			1.015
H2	Perceived Security → Trust	0.383	0.056	6.876**	Supported	0.184	0.391	0.429	1.471
H3	Trust → Intention	0.760	0.034	22.591**	Supported	0.871	0.496	0.578	1.000
H4	PP*PBE → Trust	0.077	0.024	3.136**	Supported	0.043		0.459	1.065
H5	PS*PBE → Trust	0.074	0.023	3.202**	Supported	0.023			1.053

**p< 0.01, *p< 0.05

The moderation impact of the perceived effectiveness of biometrics technologies on perceived security and trust was further analysed by plotting an interaction plot as shown in Figure 2. High perceptions of biometrics effectiveness were associated with a stronger relationship between perceived security and trust as predicted. Specifically, when perceived biometrics effectiveness was high, trust was higher even though perceived security was low. Trust was considerably better for high perceptions of biometrics effectiveness compared to low perceptions of biometrics effectiveness when perceived security was high. When perceived security was low, trust was only slightly higher for high perceptions of biometrics effectiveness compared to low perceptions of biometrics effectiveness.

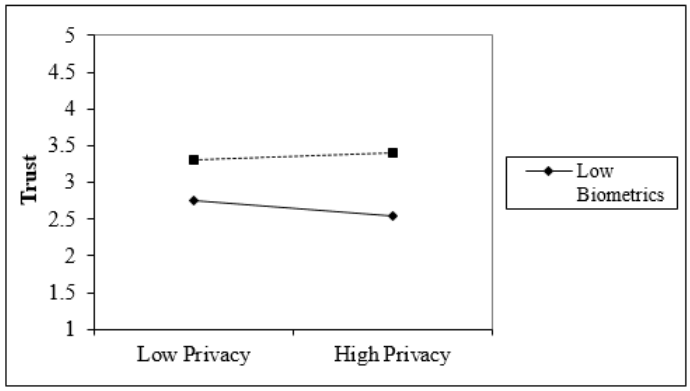
Similarly, the figure also shows that the effect of perceived biometrics effectiveness differs as a function of perceived security. When perceived security increased, trust also increased for both low and high perceptions of biometrics effectiveness. However, the increase in trust was higher for high perceptions of biometrics effectiveness compared to low perceptions of biometrics effectiveness. Therefore, perceived effectiveness of usage of biometrics technologies moderated the relationship between perceived security and trust.

Figure 2
Plot of the interaction effect between High/Low Security and Trust in Internet Banking



Perceived effectiveness of biometrics and perceived privacy showed a significant interaction in their relation to trust. However, high perceptions of biometrics effectiveness did not strengthen the relationship between perceived security and trust as predicted. Trust remained relatively high when there were high perceptions of biometrics effectiveness regardless of the level of perceived privacy. When perceptions of biometric effectiveness were low, in contrast, trust decreased as perceived privacy increased.

Figure 3
Plot of the interaction effect between High/Low Privacyand Trust in Internet Banking



The graph shows that high perceptions of biometrics effectiveness always results in greater trust than for low perceptions of biometrics effectiveness. There is an interaction because the magnitude of the difference in trust between low and high perceptions of biometrics effectiveness is different at different levels of perceived privacy. The direction of the interaction effect changes at different levels of perceived privacy. As perceived privacy increases, trust is lower when perceptions of biometrics effectiveness are low while trust is higher when perceptions of biometrics effectiveness are high. Thus, there is an interaction between perceived privacy and perceived biometrics effectiveness.

Discussion

An extended TAM model was developed in this study to investigate how biometrics technology affects trust and intention to continue using internet banking. The framework enabled examination of two important antecedents of trust in internet banking, privacy and security, and how perceived effectiveness of usage of biometrics technologies affects their relationship to trust. In addition, the large sample size in this study allowed for adequate statistical power to detect moderator effects. Therefore, the empirical testing of this model produced meaningful insights on how these constructs influenced intention to continue using internet banking.

This study was mainly designed to examine the moderating effects of perceived effectiveness of usage of biometrics technologies on the relationships between trust and both perceived privacy and perceived security. Thus, although an extended TAM model has been used as in other Internet banking studies, this study has added to existing empirical research related to Internet banking in two ways. First, the framework developed in this study is simpler than most models predicting the intention to use Internet banking. Nevertheless, a less complex model can still be beneficial as complex models result in conflicting findings due to overlaps between antecedents of trust. The relatively small framework developed enabled focus on the main constructs that have been identified in literature as important in Internet banking.

Second, although there has been an increase in research on biometrics technology, the contexts often do not relate to Internet banking. The few studies which have examined biometrics technology from an Internet banking perspective are mostly related to features of biometrics systems or acceptance of the technology (Musleh, Nofal, Ba, & Ibrahim, 2012; Dauda & Lee, 2015; Fatima, 2015). Thus far, there have been no studies examining how it moderates the relationships between constructs that are significant for Internet banking. In relation to the five hypothesized relationships in this study, statistical analysis used to test the relationships found that four hypotheses (H2, H3, H4, H5) were supported whereas one hypothesis (H1) was not supported. The following paragraphs will discuss the outcome for each hypothesis.

H1 was not supported as it was found that perceived privacy was not significantly related to customer's trust in Internet banking. The results of this study, unlike previous studies (Suh & Han, 2003; White & Nteli, 2004; Uusitalo et al., 2010; Sathye, 1999), suggest that perceived privacy might not be as important a variable as it used to be in

the past. Kim, Ferrin, and Rao (2008) found empirical evidence that security protection mechanisms were more important in affecting the behavior of customers than privacy.

The findings of this study clearly suggest that when Internet banking users perceive that privacy is high, their trust in Internet banking does not increase correspondingly. A study by (Carlos Roca, José García, & José de la Vega, 2009) on online trading systems produced similar results where they found that the relative importance of privacy concerns was lower with the presence of security features that could guarantee privacy. Thus, the absence of an effect of perceived privacy on trust could be due to customers already being comfortable disclosing personal and financial information (Carlos Roca et al., 2009). The perceived good reputation of Malaysian banks with strong privacy policies could have resulted in the embedding of confidence in privacy issues. Therefore, an increase in perceived privacy does not impact trust in Internet banking.

Consistent with previous research (Salo & Karjaluoto, 2007; Amin, 2007; YenYuen & Yeow, 2008; Kim, Steinfield, & Lai, 2008; Md Nor & Pearson, 2007), H2 was supported as there was a significant relationship between perceived security and trust in Internet banking. Therefore, the results of the present study suggest that high levels of perceived security continue to increase customers' trust in Internet banking. Specifically, an increase in perceived security will result in an increase in trust. Considering the high amounts of cyber attacks that keep increasing every year, it is probable that Internet banking customers will continue to be concerned about security issues in the future.

H3 proposed that trust is a direct predictor of intention to continue using Internet banking services. This hypothesis was supported and is consistent with other studies that provide empirical evidence for the relationship between trust and intention to use (Gefen, Karahanna, & Straub, 2003; Eriksson, Kerem, & Nilsson, 2005; Benamati, Serva, et al., 2007). According to (Eriksson et al., 2005), trust influences the intention to use Internet banking as well as other variables such as perceived usefulness and perceived ease of use. Benamati et al. (2007) found that customers' decision to use Internet banking was influenced by both trust and distrust. P. L. Yu, Balaji, and Khong (2015) provided empirical evidence from Malaysia that trust was positively associated with Internet banking continuance.

Results from the analyses examining the moderating effects of perceived effectiveness of usage of biometrics technologies on both perceived security (H4) and perceived privacy (H5) with trust showed that both hypotheses were supported. The findings contradicted studies that showed biometrics technology having a negative effect on privacy and security (Prabhakar, Pankanti, & Jain, 2003; Al Ameen, Liu, & Kwak, 2012; Mok & Kumar, 2012). Specifically, in both cases, when perceived effectiveness of biometrics technology was high, trust was at a higher level (for both low and high levels of perceived security and privacy) compared to when perceived effectiveness of biometrics technology was low. Furthermore, as perceived security increased, the increase in trust was greater for high perceptions of biometrics effectiveness compared to low perceptions of biometrics effectiveness. Although trust reduced for low perceptions of biometrics effectiveness when perceived privacy increased, for high perceptions of biometrics effectiveness, the direction of the interaction effect changed as trust increased when perceived privacy increased.

The findings suggest that perceived biometrics effectiveness is extremely important for

perceived security, perceived privacy and trust in Internet banking; consequently it can be deduced that implementing biometrics technology would lead to greater intention to use Internet banking. Although many studies have studied privacy and security as antecedents of trust, there are minimal studies that look at the role of biometrics technology as a moderator of their relationships. Malaysian Internet banking users seem open to embracing biometrics technology due to the perception that it will improve banking security and privacy. By initiating the necessary changes in Internet banking systems to accommodate biometrics technology, banking institutions can increase perceived security and perceived privacy, which should lead to an increase in trust and therefore use of Internet banking for future transactions.

Implementation of biometrics technology is still at an early stage in the Malaysian Internet banking industry. There have been new developments in the sector in terms of biometrics technology. Recently, Malayan Banking Bhd. (Maybank) raised the benchmark in Malaysian banking services by implementing a fingerprint biometrics system via a mobile application that can be used by customers to access accounts and check balances (*The Star Online Business*, 2015). The new biometric authentication speeds up access to accounts by 70% compared to the traditional mode of keying in the conventional six-digit personal identification number (PIN) (*The Star Online Business*, 2015). Since its introduction, the new system has more than 100,000 new users and has been recognised as "The Best Mobile Banking Initiative" at the Asian Banking & Finance Award 2015 (The Star Online Business News, 2015). In light of the success of the new biometric system, it is inevitable that more banking institutions in Malaysia will implement similar systems.

Future research should be aimed at the further examination of the role of biometrics technology in internet banking. There may be value, for example, in examining the perceived risks of biometrics technology in moderating the relationship between trust and intention to use internet banking. In the current study, other variables that affect trust were not selected because the objective of the study was to focus on the direct impact of perceived security and perceived privacy. Thus, it seems worth examining whether the effects of perceived effectiveness of biometrics technology would be more pronounced in the relationship of other variables with trust. Future studies could also examine whether perceived effectiveness of biometrics technology continues to affect the relationship between perceived security and privacy with trust when biometrics technology has progressed and customer experiences have changed.

Conclusion and Limitations

To conclude, this study provides researchers with the tools to discover the feasibility of biometric authentication technology in Internet banking. Empirical testing of the framework uncovered fundamental insights into the dynamics of the relationship between trust and its antecedents by incorporating user perceptions of the effectiveness of biometrics authentication technologies. Overall, the results from this study emphasize the value of implementing biometrics technology in Internet banking. Clearly perceived effectiveness of biometrics technology moderated the relationships between perceived security and privacy

with trust. These findings highlight that trust in Internet banking improves as perceived effectiveness of biometrics technology improves even when there is low perceived privacy or security. This in turn leads to greater intentions to continue using Internet banking.

Thus, biometrics technology features should be included in Internet banking system design as Internet banking users are more likely to use Internet banking when they perceive that biometrics technologies are effective. Furthermore, new solutions to enhance the privacy and security of Internet banking should utilize biometrics technology to combat the increasing number of threats to systems and users. By examining how specific aspects of biometrics technology can affect trust, perceived privacy and security, future research may reveal the types of technological improvements needed (specific hardware and software) for Internet banking. It is hoped that this study will assist regulators and banking institutions in formulating new policies and procedures to encourage implementation of biometrics technology in the banking industry to improve privacy, security and trust issues.

This study is not without limitations. Perceived security was examined as a single dimensional construct because the aim of the study was to understand the direct effect of perceptions of biometrics effectiveness on the relationship between perceived security and trust. Therefore, future research into Internet banking may include separately the dimensions of perceived security to increase knowledge about the multidimensional aspects of perceived security and the effect of perceptions of biometrics effectiveness on each dimension of perceived security.

References

Adam, N. R., Dogramaci, O., Gangopadhyay, A., & Yesha, Y. (1998). *Electronic commerce: technical, business, and legal issues*. Prentice-Hall, New Jersey.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Akhlaq, A., & Ahmed, E. (2013). The effect of motivation on trust in the acceptance of internet banking in a low income country. *International Journal of Bank Marketing*, *31*(2), 115–125.

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*(1), 93–101.

Alhussain, T., & Drew, S. (2009). Towards user acceptance of biometric technology in e-government: A survey study in the kingdom of Saudi Arabia. In *FIP Advances in Information and Communication Technology* (pp. 26–38). Retrieved from `https://doi.org/10.1007/978-3-642-04280-5_3`

Amin, H. (2007). Internet banking adoption among young intellectuals. *Journal of Internet Banking and Commerce*, *12*(3), 1–13.

Amin, H., & Ramayah, T. (2010). Sms banking: Explaining the effects of attitude, social norms and perceived security and privacy. *The Electronic Journal on Information Systems in Developing Countries*, *41*(2), 1–15.

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.

Anuar, M. M., Adam, F., & Mohamad, Z. (2012). Muslim consumers' perception on internet banking services. *International Journal of Business and Social Science*, *3*(5), 63–71.

Apostu, A., Rednic, E., & Puican, F. (2012). Modeling cloud architecture in banking systems. *Procedia Economics and Finance*, *3*, 543–548. Retrieved from `http://dx.doi.org/10.1016/s2212-5671(12)00193-1`

Arnott, D. C., Wilson, D., Mukherjee, A., & 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.

Benamati, J., Serva, M. A., et al. (2007). Trust and distrust in online banking: Their role in developing countries. *Information Technology for Development*, *13*(2), 161–175.

Ben Mansour, K., & Ben Mansour, K. (2016). An analysis of business' acceptance of internet banking: an integration of e-trust to the TAM. *Journal of Business & Industrial Marketing*, *31*(8), 982–994.

Bestavros, A. (2000). Banking industry walks 'tightrope' in personalization of web services. *Bank Systems and Technology*, *37*(1), 54–56.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211–241.

Cameron (Ed.). (2016). Skin chips. *MIT Enterprise Technology Review*.

Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management &*

Computer Security, *17*(2), 96–113.

Chin, W. W., Gopal, A., & Salisbury, W. D. (1997). Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. *Information Systems Research*, *8*(4), 342–367.

Chopra, S., & Sherry, A. M. (2014). Enhancing branchless banking technology solutions for improving consumer adoption. *Science Journal of Business Management*. doi: 10.7237/sjbm/297

Commercial banks. (27 January, 2015). Retrieved 16 June, 2016, from `http://www.bnm.gov.my/index.php?ch=li&cat=banking&type=CB&fund=0&cu=0`

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

Dauda, S. Y., & Lee, J. (2015). Technology adoption: A conjoint analysis of consumer's preference on future online banking services. *Information Systems*, *53*, 1–15. doi: 10.1016/j.is.2015.04.006

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

Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers & Security*, *14*(3), 225–231.

Eriksson, K., Kerem, K., & Nilsson, D. (2005). Customer acceptance of internet banking in Estonia. *International Journal of Bank Marketing*, *23*(2), 200–216.

Fatima, A. (2015). E-banking security issues? Is there a solution in biometrics? *The Journal of Internet Banking and Commerce*, *16*(2), 1–9.

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, *21*(6), 15–26.

Fishbein, M., & Ajzen, I. (1977). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Addison-Wesley, United States.

Flavián, C., & Guinalíu, 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., & Cha, J. (1994). *Partial least squares: Advanced methods of marketing research.* Oxford: Blackwell Publishers, United Kingdom.

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*, *9*(5), 372–382.

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

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

Gefen, D., & Straub, D. W. (2003). Managing user trust in B2C e-services. *E-service Journal*, *2*(2), 7–24.

Gholami, R., Sulaiman, A. B., Ramayah, T., & Molla, A. (2013). Senior managers' per-

ception on green information systems (is) adoption and environmental performance: Results from a field survey. *Information & Management*, *50*(7), 431–438.

Gold, A. H., & Arvind Malhotra, A. H. S. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185–214.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *30*(4), 395–410.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective*. Englewood Cliffs, Prentice Hall, New Jersey.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. (2014). Partial least squares structural equation modeling (pls-sem) an emerging tool in business research. *European Business Review*, *26*(2), 106–121.

Harby, F. A., Qahwajim, R., & Kamala, M. (2010). Towards an understanding of user acceptance to use biometrics authentication systems in e-commerce: Using an extension of the technology acceptance model. *International Journal of E-Business Research*, *6*(3), 34–55.

Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, *62*, 11–21. doi: 10.1016/j.dss.2014.02.006

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

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

Jones, L. A., Antón, A. I., & Earp, J. B. (2007). Towards understanding user perceptions of authentication technologies. *Proceedings of the 2007 ACM workshop on Privacy in Electronic Society*, 91–98. doi: 10.1145/1314333.1314352

Kim, D. J., Ferrin, D. L., & Rao, H. R. (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.

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

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford Publications, New York.

Kumar, A. (2013). *Computerworld Malaysia*. Retrieved 12 July 2013, from `http://www.computerworld.com.my/print-article/39176/`

Lallmahamood, M. (2007). An examination of individual's perceived security and privacy of the internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce*, *12*(3), 1–26.

Lee, E.-J., Kwon, K.-N., & Schumann, D. W. (2005). Segmenting the non-adopter category in the diffusion of internet banking. *International Journal of Bank Marketing*, *23*(5),

414–437.

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, *7*(2), 50–66.

Lu, H. P., Hsu, C. L., & Hsu, H. Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security*, *13*(2), 106–120.

Lupu, V. G., Catalin, & Lupu, V. (2015a). Improving the security of internet banking applications by using multimodal biometrics. *Journal of Applied Computer Science & Mathematics*, *19*(9), 37–42.

Lupu, V. G., Catalin, & Lupu, V. (2015b). Security enhancement of internet banking applications by using multimodal biometrics. In *Applied machine intelligence and informatics (SAMI), 2015 IEEE 13th International Symposium* (pp. 47–52).

Ma, Z. (2012). Factors affect the customer satisfaction of internet banking: an empirical study in China. *Journal of Convergence Information Technology*, *7*(3), 101–109.

Malay mail online. (2015). Retrieved 19 June 2014, from `http://www.themalaymailonline.com/tech-gadgets/article/malaysia-among-countries-most-hit-by-e-banking-malware-says-trend-micro`

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

Md Nor, K., & Pearson, J. M. (2007). The influence of trust on internet banking acceptance. *Journal of Internet Banking & Commerce*, *12*(2), 1–10.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*, 103–114. doi: 10.1016/j.dss.2013.05.010

Mok, S., & Kumar, A. (2012). Addressing biometrics security and privacy related challenges in China. In *Biometrics Special Interest Group, Proceedings of the International Conference* (pp. 1–8).

Morosan, C. (2010). Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: extending the technology acceptance model. *Journal of Hospitality & Tourism Research*, *36*(1), 52–84.

Musleh, M. M. M., Nofal, K. M., Ba, I. I., & Ibrahim, J. (2012). Improving information security in e-banking by using biometric fingerprint. *International Journal of Computer Science and Information Security*, *10*(3), 1–6.

Mycert. (2014). Retrieved 23 September 2014, from `https://mycert.org.my/en/services/advisories/mycert/2014/main/detail/1002/index.html`

Nasri, W., & Charfeddine, L. (2012). Factors affecting the adoption of internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior. *The Journal of High Technology Management Research*, *23*(1), 1–14.

Ndubisi, N., Sinti, Q., & Chew, T. (2004). Evaluating internet banking adoption in Malaysia using the decomposed Theory of Planned Behaviour. In *International Logistics Congress Proceeding* (pp. 2–3).

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1),

115–143.

Payment statistics. (2013). Retrieved 16 June, 2016, from `http://www.bnm.gov.my/index.php?ch=li&cat=banking&type=CB&fund=0&cu=0`

Pons, A. P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Communications of the ACM*, *51*(9), 115–118.

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

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy verification competition. *IEEE Security & Privacy Magazine*, *1*(2), 33–42.

Pranić, L., Roehl, W. S., & West, D. B. (2009). Acceptance and perceived effectiveness of biometrics and other airport security procedures. *Acta Turistica Nova*, *3*(1), 111–136.

Rajaobelina, L., Ricard, L., Bergeron, J., & Toufaily, É. (2014). An integrative model of installed online trust in the financial services industry. *Journal of Financial Services Marketing*, *19*(3), 186–197.

Ramayah, T., & Ling, K. P. (2002). An exploratory study of internet banking in Malaysia. In *Proceedings of the 3rd International Conference on Management of Innovation and Technology* (pp. 25–27).

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research*, *8*(4), 313–321.

Raza, S. A., & Hanif, N. (2013). Factors affecting internet banking adoption among internal and external customers: a case of pakistan. *International Journal of Electronic Finance*, *7*(1), 82– 96.

Raza, S. A., Qazi, W., & Umer, A. (2016). Facebook is a source of social capital building among university students evidence from a developing country. *Journal of Educational Computing Research*, 0735633116667357.

Ringle, C., Wende, S., & Becker, J. M. (2015). *SmartPLS 3.* Sage publications, California.

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.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and world wide web purchase intention. *Industrial Management & Data Systems*, *101*(4), 165–177.

Salo, J., & Karjaluoto, H. (2007). A conceptual model of trust in the online environment. *Online Information Review*, *31*(5), 604–621.

Saripan, H., & Hamin, Z. (2011). The application of the digital signature law in securing internet banking: Some preliminary evidence from Malaysia. *Procedia Computer Science*, *3*, 248–253. doi: 10.1016/j.procs.2010.12.042

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

Scott, M., Acton, T., & Hughes, M. (2004). An assessment of biometric identities as a standard for e-government services. *International Journal of Services and Standards*, *1*(3), 271–286.

Sekaran, U. (2006). *Research methods for business: A skill building approach.* John Wiley & Sons, New Jersey.

Seyal, A. H., & Turner, R. (2013). A study of executives' use of biometrics: an application of theory of planned behaviour. *Behaviour & Information Technology*, *32*(12), 1242–1256.

Sohail, M. S., & Shanmugham, B. (2003). E-banking and customer preferences in Malaysia: An empirical investigation. *Information Sciences*, *150*(3), 207–217.

The Star Online Business. (2015). Retrieved 13 July 2015, from `http://www.thestar.com.my/Business/Business-News`

Sudha, R., Thiagarajan, A., & Seetharaman, A. (2007). The security concern on internet banking adoption among Malaysian banking customers. *Pakistan Journal of Biological Sciences*, *10*(1), 102–106.

Suganthi, B. (2001). Internet banking patronage: an empirical investigation of Malaysia. *Journal of Internet Banking and Commerce*, *6*(1), 20–32.

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.

Unar, J., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, *47*(8), 2673–2688.

Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010). Trust and cloud services-an interview study. In *Cloud Computing Technology and Science (cloudcom), 2010 IEEE Second International Conference* (pp. 712–720).

Uzoka, F.-M. E., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. *Journal of Systems and Software*, *82*(9), 1550–1564.

White, H., & Nteli, F. (2004). Internet banking in the UK: Why are there not more customers? *Journal of Financial Services Marketing*, *9*(1), 49–56.

Williamson, G. D., & Money-America's, G. (2006). Enhanced authentication in online banking. *Journal of Economic Crime Management*, *4*(2), 1–42.

YenYuen, Y., & Yeow, P. H. (2008). User acceptance of internet banking service in Malaysia. In *International Conference on Web Information Systems and Technologies* (pp. 295–306). doi: 10.1007/978-3-642-01344-7_22

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in internet banking adoption. *The Service Industries Journal*, *29*(5), 591–605.

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

Yu, P. L., Balaji, M., & Khong, K. W. (2015). Building trust in internet banking: a trustworthiness perspective. *Industrial Management & Data Systems*, *115*(2), 235–252.

Yu, W. (2002). Maybank targets consumers. *News Straits Times (NST-BC)*, 2.

Zhu, R. (2015). *An initial study of customer internet banking security awareness and behaviour in China, Paper 87* (Tech. Rep.).