ADOPTION OF BIOMETRIC TECHNOLOGY

IN ONLINE APPLICATIONS

By

CHAN KOK LEONG

Research report submitted in partial fulfillment of the requirements for the degree of Master of Business Administration

2008

ACKNOWLEDGEMENT

I would like to express my deep appreciation to my supervisor, Mr Soh Keng Lin, for his guidance, enthusiasm, support and valuable advice during the process of this research and writing up of this thesis.

I would also like to thank all the respondents for this study questionnaire which provide valuable data to enable the research findings for this research. I would also like to express my thanks to my course mates, especially Khoo Kah Kheng and Fairuz Bt Muhamad Mustafa who has provide me support and advice in helping me completing this thesis.

I would like to thank my parents for giving me support and motivation in doing this thesis. Also a special thanks for my grandma for teaching me the value of hardwork and importance of education. I am grateful to my wife, Teh Ai Tee and my baby daughter, Chan Vit Ti for their loving inspiration and moral support provided throughout my research work.

Finally, I would like to thank all whose has given direct and indirect support in helping me to complete my thesis in time.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRAK

Peningkatan populariti aplikasi Internet telah mewujudkan pelbagai perkhidmatan seperti perbankan Internet, pembelian tiket kapal terbang melalui Internet dan pengisian cukai pendapatan melalui Internet untuk memberikan kemudahan and perkhidmatan yang lebih baik kepada pelanggan-pelanggan. Penipuan melalui Internet memberikan kekhuatiran yang besar dan kaedah yang lebih selamat diperlukan untuk mengenalpasti individu-individu untuk mengesahkan kemasukan mereka ke dalam aplikasi-aplikasi Internet ini. Teknologi biometrik telah semakin dilihat berpotensi sebagai penyelesaian kepada masalah tersebut (Krasnow, 2001; Chandra and Calderon, 2005; Költzsch, 2008). Namun, hanya terdapat sedikit kajian yang dilakukan terhadap faktor-faktor gunapakai teknologi biometrik di dalam aplikasi-aplikasi Internet. Ini merupakan kajian penjelajahan untuk memodelkan penentuan niat untuk menggunakan teknologi biometrik dalam aplikasi-aplikasi Internet. Dalam kajian ini, "Technology Acceptance Model" (TAM) telah diadaptasikan sebagai model asas dan dikembangkan dengan memperkenalkan pembolehubah-pembolehubah lain. Data telah dikumpulkan melalui soal selidik yang diuruskan sendiri daripada 117 responden. Hasil kajian menunjukkan anggapan kebolehpercayaan mempunyai pengaruh paling besar yang signifikan terhadap niat untuk mengguna, dan diikuti dengan anggapan senang diguna. Pembolehubah-pembolehubah lain yang didapati mempengaruhi niat untuk mengguna termasuklah inovasi peribadi, anggapan risiko terhadap teknologi baru dan kebolehan mengguna computer. Keputusan regresi hirarki menunjukkan kuasa ramalan model ini bertambah daripada 60.9% kepada 65.6% apabila pengalaman penggunaan menambahkan kekuatan perhubungan. Pengaruh anggapan kebolehpercayaan dan anggapan risiko terhadap teknologi baru akan bertambah kuat jikalau pengalaman penggunaan adalah tinggi. Kajian ini juga menunjukkan tidak terdapat perbezaan yang ketara dalam niat untuk menggunakan teknologi biometrik dalam perbankan Internet, pembelian tiket kapal terbang melalui Internet dan pengisian cukai pendapatan melalui Internet. Kefahaman mengenai kesemua faktor-faktor ini dapat membantu pembekal-pembekal perkhidmatan aplikasi Internet untuk mengatur strategi yang bersesuaian dalam perancangan dan pelaksanaan untuk menyediakan teknologi biometrik dalam aplikasi-aplikasi Internet kepada pelanggan-pelanggan mereka.

ABSTRACT

The growing popularity of online applications has led to various service offerings like Internet banking, online airline ticket purchase and online income tax filing to provide convenience and better service to customers. Online fraud is a major concern and more secure methods of identifying individuals are needed to authenticate access to these online applications. Biometric technology is increasingly being seen as a potential solution to this problem (Krasnow, 2001; Chandra and Calderon, 2005; Költzsch, 2008). However, there is little study done on the technology adoption factors on biometric technology in online applications. This is an exploratory study to model the determinants of intention to use biometric technology in online applications. In this study, the Technology Acceptance Model (TAM) is adapted as the fundamental model and extended by introducing other variables. Data was collected with a self-administered questionnaire from 117 respondents. The findings show that perceived credibility has the most significant influence towards intention to use, followed by perceived ease of use. Other variables found to influence intention to use included personal innovativeness, perceived risk towards new technology and computer self-efficacy. The hierarchical regression results show that prediction power of the model increases from 60.9% to 65.6% when usage experience moderates the relationship. Perceived credibility and perceived risk towards new technology influence on intention to use will be stronger when usage experience is high. The study also found that there is no significant difference in the intention to use biometric technology in Internet banking, online airline ticket purchase and online income tax filing. Understanding all these factors can help online application service providers to strategize their planning and implementation when deploying biometric technology in online applications to their customers.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter shall give an introduction to this study and consists of six sections. The first three sections describe the background of the study, the grounds for concern and importance of the problem. The rest of the following sections explain the implications of the research, the purpose of the research and finally the research questions.

1.2 Background of the Study

Today, there are more and more online applications that enable users to do various things anywhere and anytime via the Internet. With the worldwide access of internet, we can search for information; purchase goods and services like books and perform airline ticket booking; do financial transactions like pay bills via internet banking and online brokering to buy shares; and even deals with government agencies like submitting income tax forms and e-voting.

In the context of Malaysia, some of the popular usage includes purchasing airline tickets which were first introduced in Malaysia by AirAsia and Internet banking which are provided by various banks like Maybank, HSBC and Citibank. In year 2006, the Inland Revenue Board (IRB) tax assessment system or E-Filing was launched by the government to allow submitting income tax form via the Internet. A total of 186,343 taxpayers e-Filed their tax returns in 2006 and increased to 874,814 in 2007 (Krishnamoorthy, 2007).

However, the growing threat of the use of spyware and virus allows usernames and passwords to be stolen for unauthorized access are hampering the adoption of these online applications especially those involving sensitive data and money like financial transactions. With some analysts estimating e-commerce growth to reach $230 billion by the end of this year, online businesses are increasingly requiring ways to easily and securely identify consumers. Last year, $45 billion was lost to identity theft, indicating a high need for businesses to protect themselves, and their consumers, from risks including payment fraud, identity theft, hackers and phishing scams (Anonymous, 2008). It is not surprising that there was an overwhelming majority of consumers that are concerned about internet security as indicated by a research conducted by Washington, DC-based Frederick Schneiders Research way back in year 1999 (Daudelin, 2000).

Due to the needs to protect their customers from online fraud, extra security measures are implemented like the usage of security devices that generate a different PIN for each minute and digital certificate/signature. An example of the implementation of such security devices are by HSBC to provide protection from a variety of online attacks, including fraudulent websites, spyware and phishing/trojan horse. Meanwhile, digital certificate/signature implemented by the IRB for the E-Filing offers protection against spyware and forgery usually associated with password-based authentication.

A better security measure will be through biometric technology to validate access to the online applications. Since biometric technology utilizes certain physical and behavioral traits that are unique to an individual to identify and verify a person, it may therefore provide a better method for identification as compared to other security measures. Since a biometric device uses a unique biological trait to distinguish an individual, it is very difficult and often impossible for the identifier to be lost, stolen, duplicated, or given away (Liu & Silverman, 2001). This benefit makes biometric technology a very attractive option for companies and government agencies that want to adopt new security technology for their online applications.

1.3 Problem Statement

With the growing popularity of internet, e-commerce has gain huge acceptance with more individuals search for information, communicate, purchase and bank electronically. The Internet enables all of us to do so much more efficiently at anytime and anywhere. Organizations are relying on the Internet more heavily today than ever before to reach both their customers and partners. For the Internet savvy customer, it provides a more convenient way of accessing services and performing transactions. For the organization, it can translate into a competitive advantage as well as delivering significant cost savings versus traditional phone-based and brick and mortar transaction methods. Further, in a multi-channel environment, online services can help increase customer retention by being an effective way of delivering new products and services (Voice, 2005).

The dynamic natures of Internet with millions of computer linked to each other make it hard to control and secure the Internet environment. In all commercial spheres, the success of business has been joined hand in hand with increased fraud. The Internet has given the fraudster a new and unprecedented opportunity and means of perpetrating financial crime against businesses (Philippsohn et al., 2003). This is not surprising considering the Internet can provide the anonymity, the speed with which it operates, the ease with which a cyber criminal can get on line, and the size of the market into which to tap (with online shopping profits alone expected to exceed £103 million by 2006) (Burden et al., 2003).

According to 2007 CSI Computer Crime and Security Survey, the average annual loss reported in this year's survey shot up to $350,424 from $168,000 the previous year with financial fraud as the source of the greatest financial losses (Richardson, 2007). In Malaysia, 2003 and 2004 saw the emergence of fraudulent activities pertaining to Internet banking or better known as "phishing." A total of 92 phishing cases were reported to the Malaysian Computer Emergency Response Team (MyCERT, www.mycert.org.my) in 2004. The modus operandi of this activity is to use spoofing techniques to gain names and passwords of account holders (Mohd Zin and Yunos, 2005).

Almost every day, we can read reports on how bad the security is in the Internet. In computer security world, it is nearly impossible to keep up with the flood of detail about new viruses, worms, spam, spyware, or other attacks against computers on the network. A malicious software termed as the spyware is becoming more common. Spyware is the name of a broad class of software that collects information about activity on your computer and reports it to someone on the Internet (Treese, 2004).

With direct sales over the Internet are expected to reach $5 trillion in the United States alone by the end of this year, there is a big concern on the security issues in the Internet. Kim et al. (2008) found that Internet consumers' trust and perceived risk have strong impacts on their purchasing decisions. Consumer disposition to trust, reputation, privacy concerns, security concerns, the information quality of the Website, and the company's reputation, have strong effects on Internet consumers' trust in the Website. Another study by Salisbury et al.

(2001) claimed that security is a greater influence on intent to purchase using the Web than is the ease and utility of purchasing products.

With the growing threat of online fraud which can easily costs billions, biometric technology is seen as a way out for cyber crime. In a bid to tackle this crime, the International Biometric Group (IBG), a non-profit organisation, has conducted a number of comprehensive market reports, the latest of which covers the period up to 2007. In the report, fingerprint-based technologies, including both fingerscan and Automated Fingerprint Identification Systems (AFIS), are estimated to have accounted for $467m of 2002 industry revenue, by far the largest technology segment (Ovia, 2005).

According to Atkins (2000), biometric technologies still have some way to go before they capture the hearts and minds of the banking industry, despite developments in legislation, installations and research. There is a strong potential for growth, especially as biometric technologies fall in price and improve their image. Further, consumer understanding of the technology must be developed.

Since deployment of biometric technology involves huge amount of investment especially in online applications like Internet banking, we should learn more about the users' acceptance on this new innovation of security technology. Thus, the problem area in this study is that organizations are still not able to understand the users' acceptance of biometric technology in online applications which is relatively new especially in developing countries like Malaysia. The result in terms of savings of fraud with the biometric technology would be remarkable, but it will be a waste of money if there is no users' acceptance. Therefore, there is a need to study the factors for determining Malaysia users' intention to adopt this new security technology in the Internet.

1.4 Research Objectives

This research attempts to identify the factors that influence the intention to use biometric technology in online applications generally and also based on 3 major online application types by users in Malaysia. The online application types are Internet banking; online airlines ticket purchase and e-government services (E-Filing by IRB). This research in biometric technology will achieve its goal by using an adaptation of the technology acceptance model (TAM) for online application context. Finally, this research seeks to understand the role of usage experience as moderator on the relationship between those factors and intention to use biometric technology in online applications.

1.5 Research Questions

To achieve the objectives of this research, the following questions are addressed:

- What are the factors that influence the intention to use biometric technology in online applications by users in Malaysia?
- Does usage experience in online applications and biometric technology moderate the relationship between those factors and intention to use?
- Are there any differences in the levels of intention to use biometric technology based on types of online applications (Internet banking, online airlines ticket purchase and online income tax filing)?

1.6 Significant of Study

There is relatively little study being done to understand the users' intention to adopt biometric technology in online applications even though this is a better alternative security measure as compared to the rest of the security approaches. As such, there is an urgent need for research on this new security technology on online applications especially users' perspective on the adoption of this technology. This research will be useful to companies and governments like Malaysia and other countries that are considering the use of biometric technology in online applications to offer better protection of their users.

1.7 Definitions of Key Variables

Behavioral intention – the extent to which an individual intends to perform a specific behavior (Davis et al., 1989)

Computer self-efficacy – individual's judgement of his/her capability to use computers in diverse situation (Thatche and Perreve, 2002)

Perceived credibility - defined as the degree to which a person believe that using a particular system would be free from privacy and security threats (Ong et al., 2004)

Perceived ease of use – defined as the degree to which a person believes that using a particular system would be free of effort (Davis, 1989)

Perceived risk – perception of an individual of the adverse effect, consequences and the uncertainty that may occur by engaging in a particular behavior or activity (Dowling and Staelin, 1994)

Perceived usefulness - defined as the degree to which a person believes that using a particular system would enhance his or her job performance (Davis, 1989)

Personal innovativeness – defined as willingness of an individual to try out any new information (Agarwal and Prasad, 1998)

Usage experience – the experience of an individual in using difference types of technology

1.8 Organization of the Thesis

This dissertation consists of five chapters. The first chapter provides the background of the study, followed by grounds for concern, importance of the problem, implications of the research, purpose of the research, research questions and finally definitions of key variables. The second chapter discusses the literature review for the study which includes biometric technology, various models on adoption of new technologies, comparison of these models and extension of the new technologies models. Based on the literature review, the theoretical framework and hypotheses are developed. Chapter three covers the research methodology used for this research. Chapter four discusses data analysis and then presents the summary of the results. Chapter five is the final chapter which recapitulates the study and discusses major findings, implications and limitations of the study. It then gives suggestions for future research and the conclusion.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter consists of the literature review for this study. It starts with a description on biometric technology, followed by the explanation of various models on adoption of a new technology. The next two sections will explain the comparisons of the models and the past research done on the extensions of the technology adoption model. The review of literature leads to the development of the theoretical framework and hypotheses for this study.

2.2 Biometric Technology

The term biometrics is derived from the Greek words bio (life) and metric (to measure) (Scherer, 2005). Biometric identification exploits the universally recognized fact that certain physiological or behavioral characteristics reliably distinguish one person from another (Scherer, 2005; Ahmed and Siyal, 2005). In short, biometric is the process of automatically recognizing a person using distinguishing traits not shared by any other individuals (Harris and Yen, 2002; Scherer, 2005).

Physical characteristics include fingerprints, hand geometry, retina, iris and facial characteristics, DNA, ear and lip motion recognition (Ahmed and Siyal, 2005; Jain et al., 1999; Scherer, 2005; Langenderfer and Linnhoff, 2005). Behavioral characteristics include signature, voice, keystroke patterns and gait. (Jain et al., 1999; Scherer, 2005).

Biometric has been used throughout history. Biometrics has been applied in a variety of ways since the time of Egyptian Pharaohs who used height measurement (Davies, 1994). Babylonian kings used handprints to identify different things such as engraving (Harris and Yen, 2002). The Chinese merchants stamped children's palm prints and footprints on paper with ink to distinguish the young children from one another (Scherer, 2005).

Electronic readers have been available since the early 1970s and access is usually granted through the use of a Personal Identity Number (PIN), card or token at any entry point (Harris and Yen, 2002). However, there are many problems associated with these technologies, for example, people forget their PINs and cards get stolen by people to gain unauthorized access.

Biometric technology has its distinct features to remedy these problems. The basic aim of using biometrics is to devise a mechanism that is more secure in protecting the cryptographic key of a user as compared to the conventional method of password-based encryption (Ahmed and Siyal, 2005). Biometrics offers an increasingly attractive solution like a 'key' that the user cannot lose or forget (Gifford et al., 1999).

Gifford et al (1999) noted that the following development suggests that biometrics may experience wider spread acceptance among users:

- Greater use and more elusive computer networks - where users are now required to remember and maintain ever more PINs and passwords.
- Emerging e-commerce – internet shopping and trust service offerings require secure user verification procedures that prevent fraud and are sufficiently robust to stand up in a court of law.

Among the benefits of interest to the users as mentioned by Ahmed and Siyal (2005) are reduced risks, increased security, reduced fraud, reduced identity theft, increased convenience, enhanced service levels and increased accountability.

There is now a growing trend of biometric technology in computer especially based on fingerprint. Nowadays, there are many laptop ships with built-in finger scanners from most PC manufacturers like Fujitsu, Samsung and Sony (Stellitano, 2004; Fischer, 2007). The cost of the chips that do the fingerprint recognition has decreased considerably, driven by an increase in production volumes. As a result, it is now practical to incorporate fingerprint recognition into everyday devices (Fischer, 2007). Fingerprint readers are commercially available on laptops for about $10, and these can and have been incorporated into electronic transaction systems. For online transactions, a fingerprint reader is a reasonable and inexpensive choice for establishing security (Kleist, 2007).

In Malaysia, the early adoption of biometrics can be seen to be used in a large scale especially in airport for immigration clearance for travelers at entry and exit points for border control. The new E-passport launched in Malaysia in December 2002 is the world’s first biometrics enabled E-passport that is based on IRIS smart card technologies, combining microchip, RFID, and biometrics to secure travels documents.

Table 2.1 below listed out various biometric technologies that are used in the world today (Nanavati et al 2002; Kleist et al, 2004; Engebretson, 2005; Adams, 2006).

Table 2.1

Various Biometric Technologies Used Around the World

COUNTRY	**BIOMETRIC TECHNOLOGIES**	**PLACES**	**PURPOSE**
Malaysia	Fingerprint	Airport	Immigration clearance for travelers
USA	Iris	Prisons	Convicts identity verification before release
USA	Voice	Department of Corrections	Curfew enforcement tool for juvenile offenders
USA	Hand-geometry	Scott Air Force Base	Monitor access
Canada	Finger blood vessel pattern	Capital Direct Lending	Control entry
USA	User keystroke patterns	San Antonio City Employees FCU	User authentication for computer login

In commercial applications, Internet banking and e-commerce are two of the most important application areas due to the rapid progress in electronic transactions. Examples of applications for Internet banking include electronics fund transfer, credit card and bill payments. Some of the popular e-commerce applications include online airline ticket purchase (AirAsia, MAS), e-auctions (eBay, lelong.com.my), online cinema ticket booking (Cathay Cinema, Golden Screen Cinema) and internet retailers (Gap, Sears, Dell, Amazon).

For e-government services in Malaysia, E-Filing for submitting income tax forms online is one of the applications that have an exponential growth in terms of the number of users. However, since it is only used once a year, users might forget their digital certificates or the passwords to access the website. Hence, biometric technology is a good solution for seldom used online applications as it is usually the case for all e-government services. It allows users the convenience of accessing the website without the need to use any password.

2.3 Models and Theories on Adoption of New Technologies

There are various theories and models used in the research of adoption of new technologies, to investigate the determinants of acceptance and use of new technology. These models are based on the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975), the Theory of Planned Behavior (TPB) (Ajzen, 1985) and Technology Acceptance Model (TAM) (Adams et al., 1992; Davis, 1989; Davis et al., 1989). The determinants for the adoption of technology based on these models comes from the individual beliefs, attitudes, subjective norm, perceptions of behavioral control, perceived usefulness and its perceived ease of use.

Another model that is frequently used in information technology to explain user adoption of new technologies is Rogers' (1983) Diffusion of Innovation (DOI) theory. This model also uses behavioral intention or behavior itself as the dependent variable but the determinants are usually established according to the characteristics of the new technology such as relative advantage, complexity and compatibility.

2.3.1 Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA), proposed by Fishbein and Ajzen (1975) stated that a behavioral intention can be shaped by the attitude towards behavior and subjective norm. According to this theory, attitude towards behavior is defined as an individual's positive or negative feelings associated with a particular behavior (Fishbein and Ajzen ,1975). Fishbein and Ajzen (1975) explained that subjective norm refers to perception that most people who really matter to the individual think that he either should or should not perform the behavior in question.

2.3.2 Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (TPB) was proposed by Ajzen (1985) as an extension of the TRA (Fishbein and Ajzen, 1975) to account for situations where individuals do not have full control over their behavior by adding another construct, perceived behavioral control (PBC) for the TPB model. This construct reflects how individuals perceive the internal and external limitations to their behavior. Basically, this refers to how easy or difficult people believe it would be to perform certain behaviors (Ajzen, 1985). In TPB, behavioral intention is influenced by the attitude towards behavior, the subjective norm and the perceived behavioral control.

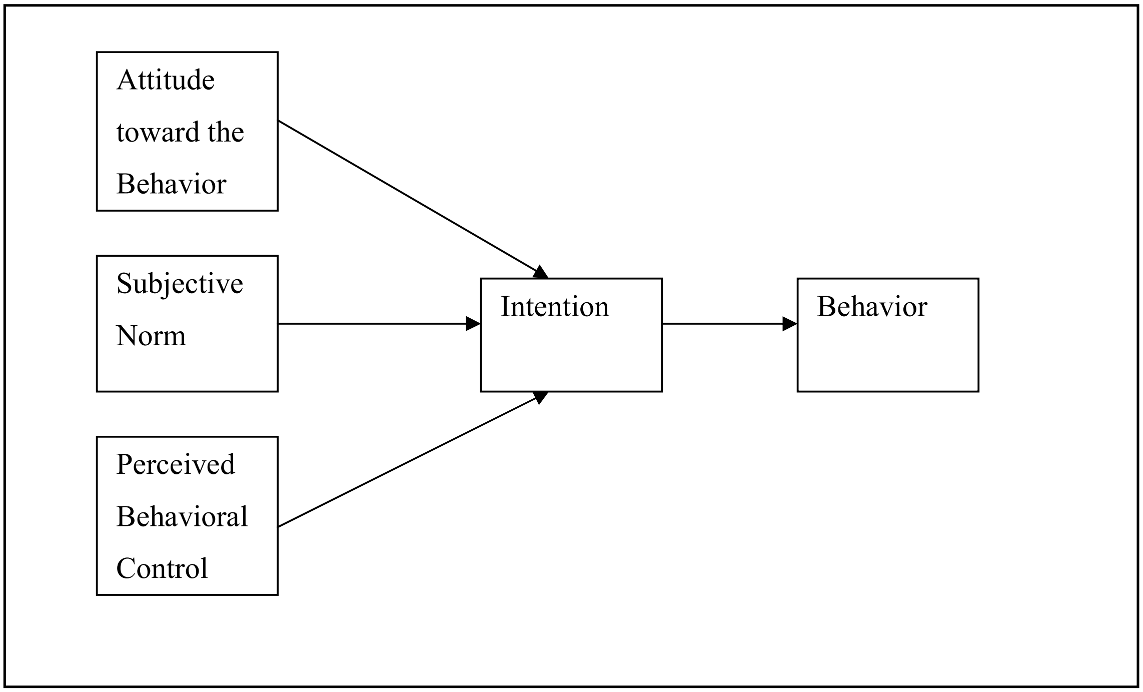

Figure 2.1 Theory of Planned Behavior (Ajzen, 1985).

2.3.3 Decomposed Theory of Planned Behavior (DTPB)

Taylor and Todd (1995) proposed a model called the Decomposed Theory of Planned Behavior (DTPB) by bringing together concepts from two distinct theories which are Diffusion of Innovation Theory (DOI) and Theory of Planned Behavior (TPB). DTPB takes three characteristics from DOI which are relative advantage, complexity and compatibility combined with perceived behavioral control from TPB.

According to Taylor and Todd (1995), DTPB offers a number of advantages because it is clearer and easier to understand the relations among beliefs, attitudes and intentions. It also enables application of the model to a variety of situations and it is more relevant in managerial conditions because it helps to determine specific factors that lead to adoption and use of new technology.

2.3.4 Technology Acceptance Model (TAM)

Applying the Theory of Reasoned Action (TRA), Davis (1989) developed the TAM for modeling of user acceptance of information technology (IT) by showing that beliefs influence attitudes about information technology, which lead to intentions and subsequently behaviours of actual technology usage. Davis (1989) has shown that perceived usefulness and perceived ease of use of the technology influenced the beliefs that lead to system usage. Based on TAM, the greater the perceived usefulness and the perceived ease of use, the better is the individual interests towards the new technology and the higher the intention to adopt it.

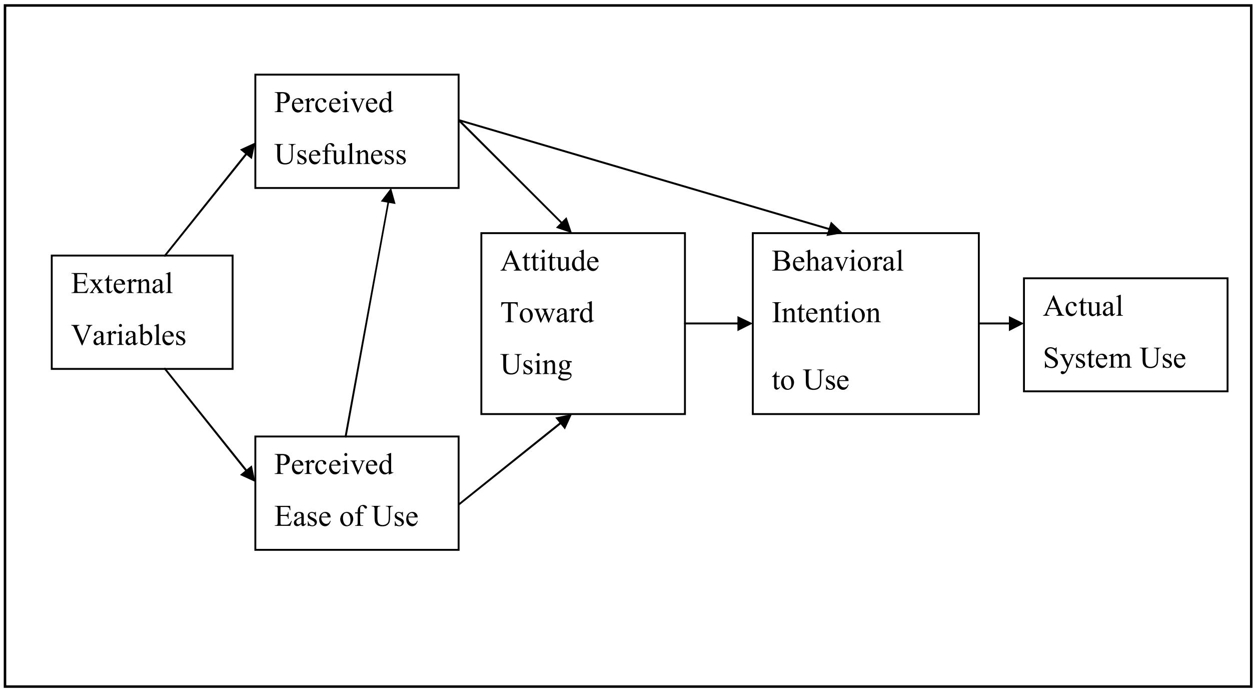

Figure 2.2 Technology Acceptance Model (Davis et al., 1989).

Many studies have used TAM to evaluate user adoption of various information technologies like e-commerce (Lee et al., 2006; McKechnie et al., 2006), e-government

(Schaupp and Carter, 2005; Belanger and Carter, 2008), Internet banking (Wang et al., 2003; Pikkarainen et al., 2004, Guriting and Ndubisi, 2006; Yiu et al., 2007), mobile banking (Luarn and Lin, 2004), mobile commerce (Yang, 2005; Wu and Wang, 2004), e-learning (Liao and Lu, 2008; Saade and Bahli, 2005; Ong et al, 2004), open source software (Gallego et al, 2007), mobile credit card (Amin, 2007) and internet tax-filing systems (Chang et al, 2005; Wang, 2002).

Chan et al. (2005) claimed that TAM proves to be a valid model to explain the taxpayers' acceptance of the Internet tax-filers' system. Guriting and Ndubisi (2006) found that perceived usefulness and perceived ease of use are strong determinants of behavioral intention to adopt online banking. It is similar with the findings by Yiu et al. (2007) on their study on Internet banking in Hong Kong. A study by Lee et al. (2006) found that perceived usefulness, perceived ease of use and perceived enjoyment, significantly enhanced consumer attitude and behavioral intention towards an online retailer.

.

2.3.5 Diffusion of Innovation (DOI)

The Diffusion of Innovation theory is useful to explain the process of innovation adoption. The individual's decision on whether to use the technology is based on the following five characteristics that consistently proved to be determinants of the diffusion rate of an innovation (Rogers, 1983). They are:

(1) Relative advantage and it refers to the extent to which the innovation is perceived as superior to all other options.

(2) Compatibility and it refers to the extent to which the innovation is perceived as being in line with the values, needs and experiences of prospective adopters.

(3) Complexity and it refers to the extent which the innovation is perceived as difficult to understand or use.

(4) Observability and it refers to the extent to which the benefits or attributes of the innovation can be observed, pictured or described to prospective adopters.

(5) Trialability and it refers to the extent which the innovation can be experienced before its actual adoption.

The relationship between each of these characteristics and the intention to adopt the new technology is positive, except the complexity attribute, which shows a negative relationship to the intention to adopt.

2.4 Comparisons of Models and Theories

All the models and theories (TRA, TPB, DTPB, TAM, and DOI) contain the same independent variable, which is the intention to use. TRA dependent variables are attitude towards behavior and subjective norm. By adding perceived behavioral control to TRA, we have TPB.

TAM dependent variables are on perceived usefulness and the perceived ease of use. DOI dependent variables are somewhat overlapping with TAM dependent variables. They are perceived usefulness in TAM and relative advantage in DOI, and perceived ease of use in TAM and complexity in DOI. Based on that, by adding compatibility, observability and trialability to TAM, we will have DOI. By combining three characteristics of DOI (relative advantage, complexity and compatibility) with perceived behavioral control from TPB, we have DTPB.

Recently, many researches are done extensively based on TAM or via the extension of its model for various technologies adoption in different countries such as Internet banking in USA, Taiwan, Brazil and Finland (Curran and Meuter, 2005; Hernandez and Mazzon, 2007; Wang et al, 2003; Pikkarainen et al, 2004), mobile credit card in Malaysia (Amin, 2007), e-government in UK (Gilbert et al., 2004), electronic healthcare in Norway (Lanseng and Andreassen, 2007), online retailer in USA and UK (Lee et al, 2006; McKechnie et al, 2006), e-voting in USA (Schaupp and Carter, 2005), internet usage in Singapore and India (Teo, 2001; Fusilier and Durlabhji, 2005), information systems in Malaysia (Ndubisi and Jantan, 2003), mobile internet in Korea (Cheong and Park, 2005) and online music purchase in Taiwan (Chu and Lu, 2007).

Researches done based on DOI are usually combined with TAM (Gilbert et al., 2004; Schaupp and Carter, 2005). It is also similar for research based on TPB (Fusilier and Durlabhji, 2005). Shih and Fang (2004) used DTPB as the model for Internet banking in Taiwan. Other than that, researches are also done based on the integrated model approach, such as combining TAM and DTPB (Hernandez and Mazzon, 2007; Thompson et al, 2006).

2.5 Extension of the Existing Technology Adoption Models

As technology has continued to transform continuously especially on the Internet applications, many extensions of the models, especially from TAM have been proposed. Studies have been done by introducing other dependent variables such as perceived risk (Lu et al, 2005; Curran and Meuter, 2005; Walker and Johnson, 2006; Cunningham et al, 2005; Lee and Allaway, 2002), trust (Lanseng and Andreassen, 2007; Schaupp and Carter, 2005; Wu and Chang, 2005), experience with technology (McKechnie et al, 2006; Cheong and Park,

2005) and computer self-efficacy (Ndubisi and Jantan, 2003; Wang et al, 2003; Thompson et al, 2006).

2.6 Theoretical Framework

This theoretical framework for this study is described in this section.

2.6.1 Gap in the Literature

Although there are extensive studies of various technologies like Internet banking, online purchase and government e-services employing various technology adoption models like TAM and DOI, there is very little literature concerning the adoption of biometric technology in online applications. Thus, the research here will focus on the adoption of this new technology.

2.6.2 Research Model

The dependent variable for this research is the intention to use biometric technology in online applications. The actual usage is not used as the dependent variable since there is little of this technology that is in use in Malaysia. Similar in many other studies of TAM with the extended model (e.g., Adams et al., 1992; Wang et al., 2003; Fusilier and Durlabhji, 2005; Luarn and Lin, 2005), the attitudes construct has been removed to simplify the model. Based on the literature review, TAM is able to explain and offer a better prediction on the users' intention to use a new technology. As such, this research uses selected constructs from TAM (Davis et al., 1989) which are perceived ease of use (PEOU) and perceived usefulness (PU) as the independent variables.

Since TAM was created to explain the factors of Information System (IS) acceptance, other independent variables are included in this study of adoption of biometric technology in online applications. The other independent variables are perceived risk and perceived credibility (Wang et al., 2003), personal innovativeness (Yang, 2005; Thompson et al, 2006; Yiu et al., 2007; Crespo and Rodrıguez, 2008) and computer self-efficacy (Ndubisi and Jantan, 2003; Wang et al., 2003; Thompson et al, 2006). This study also included usage experience as a moderator variable.

Hence, the following model as shown in Figure 2.3 is developed for this research.

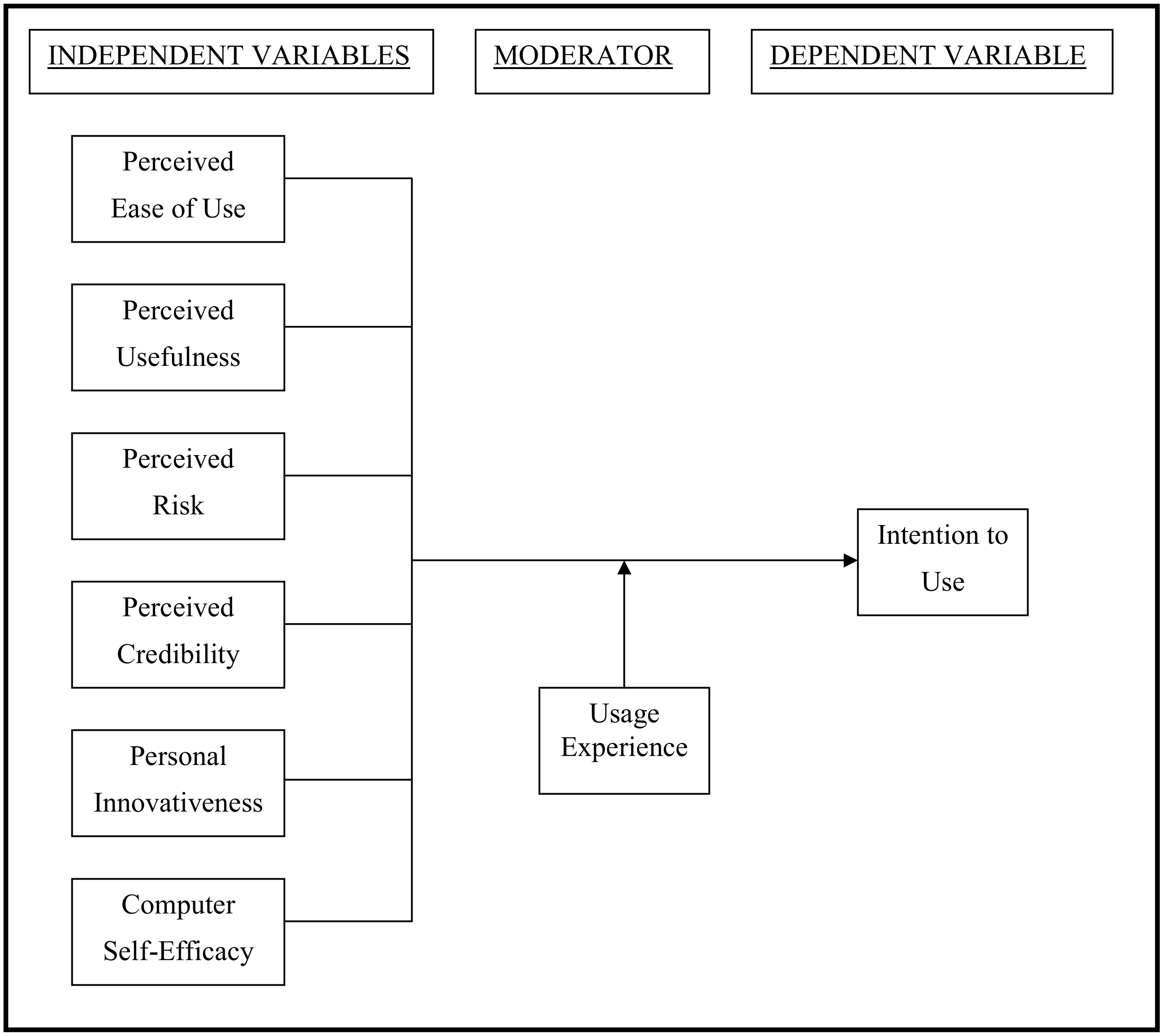

Figure 2.3 Research Model.

2.7 Hypotheses Development

This section describes the hypotheses development based on the research model.

2.7.1 Perceived Ease of Use (PEU)

Perceived usefulness and perceived ease of use are the elementary variables for TAM. Perceived ease of use refers to the degree to which a person believes that using a particular system would be free of effort (Davis, 1989). Extensive research over the past decade provides evidence of the significant effect of perceived ease of use on usage intentions. It was found that perceived ease of use has a positive effect on the behavioral intention to use Internet banking in Taiwan (Wang et al, 2003). This means users are more likely to adopt Internet banking if it is easy to use.

The study done by Amin (2007) conducted in Labuan and Sabah, Malaysia has shown a significant impact of perceived ease of use on the intention to use mobile credit card. The results generally support the findings of the positive effect on perceived ease of use on the intentions to use other technologies like electronic healthcare (Lanseng and Andreassen, 2007), online retailing of financial services (McKechnie et al., 2006) and biometric devices (James et al., 2006). Based on these findings, it is likely that the general relationship found in TAM is also applicable to biometric technology in online applications. Thus, based on these findings, the following hypothesis is developed:

H1. Higher levels of perceived ease of use will be positively related to higher levels of intention to use biometric technology in online applications.

2.7.2 Perceived Usefulness (PU)

The second variable in the TAM construct is perceived usefulness. Davis (1989) defined perceived usefulness as the degree to which a person believes that using a particular system would enhance his or her job performance. There is considerable research in the information system (IS) area that provides evidence of the significant effect of perceived usefulness on usage intentions on various internet applications (Lu et al., 2005; Pikkarainen et al., 2004; Schaupp and Carter, 2005). It was found that perceived usefulness positively influences the acceptance of online antivirus applications (Lu et al., 2005) and online banking (Pikkarainen et al., 2004). These results are consistent with the findings on government online applications by Schaupp and Carter (2005) who found that perceived usefulness has a positive effect on the usage intentions of e-voting.

The inclusion of this variable in this study is that Malaysian users take advantage of the biometric technology in online applications because it is useful to make login easier and more quickly. Thus, perceived usefulness is eligible to be applied in this research. The following hypothesis is hence developed:

H2. Higher levels of perceived usefulness will be positively related to higher levels of intention to use biometric technology in online applications.

2.7.3 Perceived Risk (PRISK)

Previous researches have indicated that perceived risk impact intentions to use an online applications (Lu et al, 2005; Walker and Johnson, 2006; Curran and Meuter, 2005; Cunningham et al, 2005). Firstly, perceived risk may be associated with the technical performance or functional reliability of the online delivery system. Secondly, perceived risk may be associated with personal privacy and security.

Since there is no face to face interaction, users might perceive higher security risk especially associated with unauthorized access in online transactions. As such, perceived risk is also one of the significant factors in online applications like Internet banking. This was demonstrated in a study done by Curran and Meuter (2005) who found that perceived risk was found to have a significant impact on the adoption of online banking but no significant impact for ATM and banking by phone.