# Modelling User Trust and Mobile Payment Adoption: A Conceptual Framework

Uchenna Cyril. Eze, Multimedia University, Melaka, Malaysia, uchenna.eze@mmu.edu.my

Gerald Goh Guan Gan, Multimedia University, Melaka, Malaysia, gggoh@mmu.edu.my

John Ademu, Multimedia University, Melaka, Malaysia, jonpinjeff@yahoo.com

Samson A. Tella, Multimedia University, Melaka, Malaysia, sa_tella@yahoo.com

***Abstract***

*The proliferation of new technologies and the changing dynamics of industry competition have spurred growth in innovative production, marketing and consumption. The need for convenience has also fuelled enormous interest in the use of mobile payment innovations, which in turn creates security challenges for users. Indications are that mobile phones and handheld devices should have made more inroads in businesses and societies as in most advanced societies are at today [1]. Instead, there has been a slow acceptance of mobile and handheld devices as alternative payment systems, especially in developing countries, despite the efforts of key players such as banks, mobile network operators, and mobile payment service providers (MPSP). This paper, therefore, is a conceptual design to examine security factors influencing the acceptance of mobile payment systems in Malaysia. This paper will examine the impact of security dimensions on trust and how these impacts on trust influence users' intention to use mobile payment systems. We will also highlight several research, practitioner and policy implications.*

Keywords: Mobile Payment, Security, Conceptual Model, Trust

## 1. Introduction

According to recent research findings and forecasts in business, media and academia, mobile phones and handheld devices should have been firmly established as an alternative form of payment in most technologically advanced societies [1]. Despite ongoing efforts by key players such as banks, mobile network operators and mobile payment service providers (MPSP) in promoting and offering mobile payment options, absence of widespread customer acceptance of this innovation have resulted in a lag in the adoption of mobile payments as an alternative form of payment mechanism [1]. While each of these players approach the market with different expectations, several studies have shown that merchant/consumer adoption is key to the success of mobile payments [1, 2].

'Mobile payments are defined as the use of a mobile device to conduct a payment transaction in which money or funds are transferred from a payer to a receiver via an intermediary or directly without an intermediary' [3]. Due to the all-encompassing nature of this definition, it should be made clear that a distinction exists between mobile payments and mobile banking. The latter refers to mobile payment transactions that are exclusive to their respective customers whilst the former is a mode of payment that is widely available to all parties in a retail environment [3]. Mobile payments have been suggested as a solution to facilitate micropayments in electronic and mobile commerce transactions and to encourage reduced use of cash at point-of-sales terminals [3, 4]. If efforts in promoting the use of mobile payments succeed, it will boost both e-commerce and m-commerce adoption and may be the killer service in 2.5G, 3G and beyond [2].

The early development of mobile payment was largely triggered by the high penetration rate of mobile phones and handheld devices in most markets. Mobile phones today clearly outnumber every other mobile device. In 2004, the Gartner Group predicted that by 2008 there will be more mobile phones worldwide than televisions, fixed line phones and personal computers (Gartner, 2004). Recent statistics from the Malaysian Communications and Multimedia Commission [5] show that there are more than 23,347,000 mobile phone subscribers in the Malaysian, with a penetration rate of 85.1%. The AT Kearney Global Outsourcing Survey has ranked Malaysia at the third highest position globally because of its attractiveness as a mobile content and applications centre.

Despite the high penetration rates, a national survey of mobile phone users conducted by the Malaysian

Communications and Multimedia Commission in 2006 revealed that only 17.6% of mobile phone users had actually purchased products or services using their mobile phones [6]. Recent examples of not too successful uptake of electronic payment systems indicate that better understanding of the adoption of payment systems by consumers is needed to guide future development of Mobile Payments [3].While this issue has been raised in several studies, most of these studies are exploratory and there is limited data on the adoption of mobile payment systems by consumers, more so for the Malaysian scenario.

This study analyzes the complex environment of mobile payments and focuses on examining consumer willingness to use mobile phones as a payment instrument in transactions where money is transferred from consumer to merchant in exchange for products or services. It is pertinent to stress that several electronic payment schemes have failed to achieve the much desired critical mass required. Well known cases of failures include eCash, ePurse and some other electronic smart card schemes [7]. Most schemes failed because the focus of awareness campaigns were based largely on technical aspects that were of little importance to customers. There is a need to make sure that security issues are adequately addressed and designed in alignment to the subjective perceptions of potential consumers [7]. To our knowledge, there are currently no findings from an empirical survey of consumer perceptions on mobile payment in Malaysia. As such, this paper aims to examine the extant literature on the role of security in the adoption of mobile payments amongst mobile phone users in Malaysia. This study will explore the drivers, determinants and factors of security that may affect consumer adoption of mobile phones as an alternative means of payment by proposing a conceptual model that examines trust and mobile payments adoption.

## 2. The Mobile Payment Arena

Today's mobile payment arena is non-standardized with major players approaching the market with their own proprietary infrastructures and solutions. Concerning payment models, there currently is no widely accepted, dominating or standardized mobile payment model. There are about four existing mobile payment models i.e. acquirer-centric, user-centric, bank-centric and mobile network operator centric models. Karnouskos [2] states that the most likely dominant players in the arena would be banks and mobile network operators (MNO). He foresees a movement towards composite models where the main players cooperate on a revenue sharing basis.

Most payment transactions consist of three basic phases. First the consumer chooses the desired product by shopping. After the shopping phase, the customer is billed by the merchant. Finally, the customer pays the merchant for the good. According to Ondrus and Pigneur [8], there are many possibilities of extending the number of phases during a payment transaction. The most pertinent issue is that the transaction must be easy to use to the customer regardless of how complex the transaction may be. The mobile payment scenario currently has several proprietary models in terms of transaction scenarios.

## 3. Categorization of typical mobile payment procedures

While the key phases of the generic mobile payment procedure is applicable to almost all transactions, they can be categorised into several different groups or procedures based. Karnouskos [2] categorises mobile payment procedures them as location-based (remote and proximity Transactions), value-based (micro-payments, mini-payments and macro-payments), charge-based (post-paid, pre-paid and pay-now), validation-based (online mobile payment, offline mobile payment) and technology-based (single chip, dual chip, dual slot), token-based (e-coin) and account-based (wireless wallets).

Location of purchase has been the key determinant in driving various forms of electronic payments as evidenced in several studies. Mobile payment is expected to further drive the market with the introduction of new features. Mobile phones have been used as wallets in several payment scenarios. Nokia and Master Card have conducted several joint tests since 2003. Proximity payments usually involve two parties using an ad-hoc network based on wireless technologies such as Bluetooth, infrared and radio frequency identification (RFID) which enable short-range wireless device to device payments.

Recently there have been research and developments into a new technology called near field communications (NFC). NFC is a short-range wireless technology like RFID tags, which are used to track stock by retailers. The tags inside phones could have personal information stored in them and could act as car keys, money, tickets and travel cards. Mobile firms representing 40% of the global mobile market back NFC. The potential inhibiting factors may be the risks involved like non-repudiation.

## 4. Factors influencing the adoption of mobile payments

The diffusion of innovations theory has played an important role in providing a theoretical framework for the study of information technology adoption by both individuals and organisations. Using the diffusion of innovations theory proposed and later refined by Rogers (1995), numerous models and frameworks have emerged to address the adoption of information technology and its related applications. Many of these models analyse the behavioural aspects of the adopters such as perception, attitude and motivation, often integrating diffusion of innovations literature with other theories or models.

Among the models that have been developed to provide an understanding of usage and adoption of information technology is the Technology Acceptance Model [9] which is grounded in models from social psychology such as the Theory of Reasoned Action (TRA) [10] and Theory of Planned Behaviour (TPB) [11]. TAM is at present a pre-eminent theory of technology acceptance in information systems research. Numerous empirical tests have shown that TAM is a robust model of technology acceptance behaviours in a wide variety of IT-related fields [12].

TAM originates from TRA [10] and proposes a behavioural model where two beliefs - perceived ease of use and perceived usefulness are the primary predictors of use intentions. TAM postulates that these two beliefs determine the attitude toward using the system and that attitude, together with perceived usefulness, determines use intention. Use intention then predicts the actual system use [12].An extensive body of research has demonstrated the explanatory power of TAM in predicting use of various information technologies such as word processing software, World Wide Web use and Internet shopping.

According to the TAM, perceived usefulness (PU) is defined as “the degree to which a person believes that using a particular system would enhance his or her job performance” and perceived ease of use (PEOU) is defined as “the degree to which a person believes that using a particular system would be free of effort” [9].Both constructs influence one’s attitude toward system usage, which influences one’s behavioural intention to use a system, which, in turn, determines actual system usage. Some studies already underlined the importance of the criteria perceived usefulness and perceived ease of use for mobile payment acceptance [3]; [12].

TAM has proven to be a useful theoretical model in helping to understand and explain use behaviour in information system implementation. Researchers have simplified TAM by removing the attitude construct found in TRA from the current specification. The proposed research model to examine the role of security in mobile payment adoption is based on the generic constructs of the TAM. TAM provides the theoretical framework upon which the various constructs are being examined and evaluated.

Attempts to extend TAM have generally taken one of three approaches: by introducing factors from related models, by introducing additional or alternative belief factors, and by examining antecedents and moderators of perceived usefulness and perceived ease of use. Mallat [3] suggest the need for acceptance models which are tailored to specific technologies. They argue that generic models may not be adequate enough to explain the adoption and use of different types of technologies and service channels where specific features of the technology may play an important role. Therefore, it is important to include other explanatory variables into TAM [12]. Relating to the specific nature and uniqueness of mobile payment adoption, six key variables have been included in the model. These variables are confidentiality, authentication, non-repudiation, integrity of data, authorization and trust that are hypothesised as affecting the perceived security of mobile payments and its eventual adoption.

## 5. Mobile payment security

Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing. These technologies are needed to address various payment industry needs, which includes, Secure authentication infrastructure on mobile devices, secure transmission infrastructure for wireless payment, trust/validation directories and virtual “wallets” stored on a mobile device or accessible over a network [1].

Security is both an enabling and disabling technology. Its purpose is to enable communications and transactions to take place in a secure environment without fear of compromise, while at the same time disabling non-legitimate activities and access to information and facilities [8, 13, 14]. Non-legitimate activities include eavesdropping, pretending to be another party (also known as impostering or spoofing), or tampering with data during transmission. In general these activities are either unacceptable or illegal outside of the digital environment, so security simply helps to enforce the status quo in that sense [8, 13, 14].

Previous studies on security issues in the IS arena have been mainly focussed on technical and implementation-based issues. However, most consumers only perceive security from the subjective realm. This is generally incubated through advertisements and public information [2].The security of most existing mobile payment schemes is not too strong and has not been widely exploited due to the infancy of this application. When mobile payments reach a critical mass, and the manipulation of such services results in economic benefit, there will be organized efforts to compromise mobile payments and incur serious losses on the part of both merchant and consumers [8, 13, 14]. Typically, security levels relating to mobile payment do not match the standards required by a bank or card issuer in order for them to assume the risk of payment. There is also the common end-user perception that many mobile payment solutions are fraught with insecurities.

Although the issue of security has emerged as a major inhibitor of mobile payment acceptance, the research on this issue is quite rare to date, especially from the viewpoint of customers. Security and privacy concerns of transactions are not novel concepts. Hence, Shneiderman [15] argues that improving positive security and privacy perceptions are most important for sustained activity in electronic commerce and more importantly mobile payments. Chari, Kermani, Smith, and Tassiulas [16] argue that mobile commerce solutions differ from electronic commerce solutions because the underlying technology has basic differences which create a range of new security exposures. For instance, the portability of mobile devices makes theft, loss, and damage of client devices much more likely. Therefore they assume that also the perception of security in mobile commerce may differ from that one in electronic commerce.

## 6. Dimensions of mobile payment security

Some of the available research into mobile payment adoption has shown that lack of perceived security is one reason for inhibition as indicated by Mallat [3] who conducted a study using focus groups. Khodawandi, Pousttchi and Wiedemann [17] have attempted to conduct empirical research into subjective security. In general, there is very little analysis on a broad range of security requirements based on the Technology Acceptance Model (TAM) that has been applied specifically to mobile payments.

The concept of security has been split into relevant dimensions by researchers. They define security in the context of objective and subjective security. Objective security is a concrete technical characteristic. Egger and Abrazhevich [18] explain that it is unlikely that the average customer is able to evaluate the technicalities of objective security. Hence, subjective security which is defined as the degree of perceived sensation of the procedures' security from the view point of the consumer is argued to be a more pertinent measure to gauge how mobile payment security affects consumer adoption [18]. As such, this study will emphasise on the subjective security perceptions of mobile payment among consumers in Malaysia as this innovation is expected to make inroads in Malaysia in the not too distant future.

It is important to adopt the appropriate level of security, which will allow organizations to take full advantage of the business opportunities while at the same time giving consumers confidence in the security of the service. End users must trust the payment service provider behind the solution [14, 19]. Bauer [20] first proposed that consumer behavior be seen as risk taking, valuable empirical researches have attempted to identify various types of perceived risk in the context of consumers' purchase behavior. The risk of information theft and corruption of data is a growing reality in many electronic payment schemes. These vulnerabilities may be inhibiting factors in mobile payment adoption. Security breaches can result in invasions on privacy and financial loss [18]. Emerging mobile payment service providers and key players could suffer from bad image and litigations resulting from these security breaches. Hence, the security requirements of confidentiality, integrity, authentication, authorization and non-repudiation are critical to the attainment of both subjective and objective security of mobile payments [18].

## 7. Trust in mobile payments

Consumer perceptions of security have increased lately, even in the face of advances in security technologies. These concerns may lead to distrust in mobile payments security. Studies conducted of cellular phones revealed large numbers of cellular phone frauds, resulting in low user trust of the technology therefore hampering adoption rates. The concept of trust has received several definitions by researchers. In many studies, trust is based on previous interactions [21]. According to [22], trust has three characteristics: competence, benevolence and integrity. McKnight and Cheverney [23] added the characteristic of predictability. Trust is the foundation of most financial transactions and is built on a multitude of factors such as the consumers' perception of the security of the mobile payment system. Studies show that user perceptions of control are an important ingredient of transaction trust. Ondrus and Pigneur [8] posit that a high level of trust in mobile payments is more of a basic requirement than a competitive advantage especially when fraudulent activities are frequent and financial risks are high.

*Confidentiality*

The information must not be disclosed to unauthorized persons, processes or devices. It is assumed that only the sender and receiver are able to comprehend the transmitted messages in clear text. This is usually accomplished using computer based cryptographic encryption. The major attacks on confidentiality are traffic analysis, eavesdropping, and man-in-the middle attack. Customers care about how a mobile payment procedure is protected against passive monitoring of payment details. According to Merz [24],confidentiality is the property of an information system that ensures that transaction information cannot be viewed by unauthorized persons.

H1. Perceived strength of **confidentiality** would have a positive impact on a consumer's **trust** in mobile payments.

*Integrity*

Integrity means that the information and systems have not been altered or corrupted by external & unauthorized parties [24]. Adding secure electronic signatures to messages provides transaction data integrity. Attacks on integrity include session hijacking, replay attacks and man-in-the middle attacks. An integrity threat exists when an unauthorized party can alter message stream of information [24]. Unprotected transactions are subject to integrity violations. Those businesses that participate in the payment system absolutely must protect their customers' data. This is a promise, a responsibility, and increasingly, a customer expectation [25]

H2. Perceived strength of **integrity** of data would have a positive impact on a consumer's **trust** in mobile payments.

*Authentication*

This ensures that the parties to the transaction are not impostors and are trusted [24]. Before business transactions can be performed, the participating entities must confirm the identity of each other. This is achieved by using network based authentication protocols and PIN. The attacks on authenticity are also session hijacking, replay attacks and man-in-the middle attacks [24]. Authentication from the consumer means obtaining a level of comfort with a claimed identity [24]. The level of comfort is likely to vary with the value of the transaction and the risk it represents. Security concerns, with respect to exposure of credit card information to hackers or unknown vendors are still a major anxiety for consumers.

H3. Perceived strength of a**uthentication** would have a positive impact on a consumer's **trust** in mobile payments.

*Authorization*

Procedures must be provided to verify that the user can make the requested purchases [24]. This is usually ensured by the use of PIN and Passwords to validate the authority of the provider to the services or transactions requested to be performed.

H4. Perceived strength of **authorization** would have a positive impact on a consumer's **trust** in mobile payments.

*Non-repudiation*

This ensures that a user cannot deny they performed a transaction. The user is provided with a proof of the transactions and recipient is assured of the user's identity [24]. This is achieved by digital signature techniques. These procedures involve a variety of policies and processes along with hardware and software tools necessary to protect the systems and transactions. Many business transactions over the Internet involve the exchange of digital products between two parties – electronic mails, digital audio and video, electronic contract signing and digital signatures, to name a few. Often these transactions occur between players that do not trust each other [24]. Bhimani [26] states that consumers may be afraid that online vendors can deny an agreement after the transaction.

H5. Perceived strength of **non-repudiation** would have a positive impact on a consumer's **trust** in mobile payments.

The Theory of Reasoned Action by Fishbein and Ajzen [10] asserts that attitude toward a behaviour is determined by relevant beliefs. Gefen [21] defines trust as a confident belief in favourable expectations about what the other party would do. Trust is therefore pertinent in unfamiliar terrains and zones of transactional uncertainty like mobile commerce and mobile payments.

H6. **Trust** would have a positive impact on a consumer's **intention** towards using mobile payments for transactions.

Several researchers in marketing and the social sciences have empirically verified causal relationships between trust and behavioural intentions. Ganesan [27] showed that trust is a necessary ingredient for long term orientation because it shifts the focus to future conditions. Ganesan scientifically validated that trust in a supplier, in the case of mobile payments, is central to a consumer's intention to continue a relationship and would therefore be anticipated to positively impact on the users' intention to use mobile payments for their transactions.

Davis et al. [28] adopted the Theory of Reasoned Action's causal relationships in the Technology Acceptance Model (TAM) to explain the adoption behaviour of individuals in relation to information systems. This study shall also follow their cue and apply the model in the domain of the adoption of mobile payments. Using the TAM as the framework for this study, a conceptual model of user trust and mobile payment adoption is presented in Figure 1, which encompasses the key factors in ensuring user trust of mobile payment and the posited resulting outcomes of intention to use mobile payments and actual adoption of mobile payments.

We will also examine other paths in the model [Figure 1] including the paths between Trust and Perceived ease of use, Trust and perceived usefulness, Perceived ease of use and intention to use and Perceived usefulness and Intention to use.

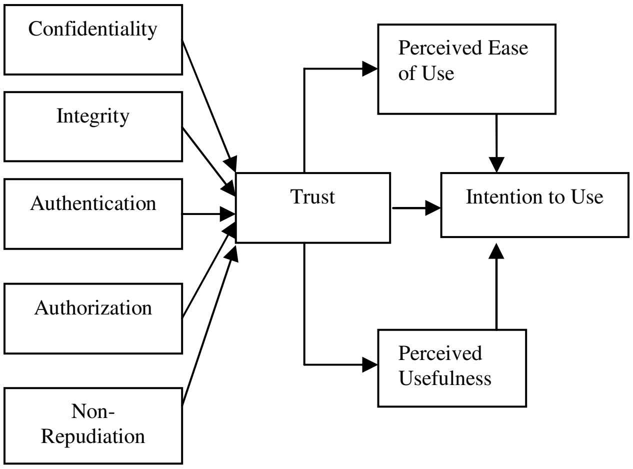

*Fig 1. Conceptual model of user trust and mobile payment adoption*

## 8. Research Method

We will develop a survey questionnaire for this study. The questionnaire will be designed based on the research conceptual model (see Figure 2). Items will be adapted from prior works on innovation deployment and diffusion related to the concepts this paper advances as discussed in the earlier sections. Responses to the survey questions will be entered on a Five-point Likert-type scale as follows: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. The survey questionnaire will include data on participants' profile: sex, age, combined household income, education, job position, family size, and the ethnicity of participants.

We will select the sample of about 600 potential mobile payment device users for this study using convenience sampling method because this study focuses on consumers' perspective and there is no population frame to enable random sampling process. The target population will be residents in Malacca, Malaysia, using mobile devices and who intend to use these devices as future payment tools. Residents in Malacca may be locals or foreigners who are studying or working in Malaysia. This is to ensure that those who participate in this study are not in transit or are in Malaysia for a short visit, say, less than three months.

We will then take several steps to ensure data validity and reliability. Initially, the questionnaire will be pre-tested with two academics resident in Malacca and two academics resident outside Malacca. The questionnaire will then be revised for any potentially confusing items, before the administering the pilot survey. A pilot survey is aimed at providing an opportunity to objectively measure validity and reliability of the questionnaire [29, 30]. Based on the above recommendations, a pilot study for this research is necessary in developing the survey questionnaire. The pilot study will be conducted using a selected group of 20 residents in Malacca. The suggestions and comments from the pilot study will be evaluated, and those considered relevant will be incorporated into the survey or test design prior to the actual study. We will then use personal questionnaire administration to collect data for this research.

To establish the absence of non-response bias, it is desirable to collect data from a set of non-respondents and compare it to data supplied willingly. For a meaningful number of surveys and for all survey items, this method is rarely achievable. A practical preference, that has been argued to provide reliable results, is to compare the mean values of responses for earlier returns with the means from later returns [31]. This approach has the capacity to reveal any differences between early and late responders who required prompting. The assumption is that late responders share similarities with non-responders, and if no significant differences exist, the probability is strong that non-response bias does not exist [32]. We will conduct tests for all the constructs between first week respondents and those who responded after five weeks, and then determine the differences between the two groups.

## 9. Data Analysis Techniques

Multiple research techniques will be used in this study including descriptive techniques, factor analysis, multiple linear regression, t-test, analysis of variance (ANOVA), Structural equation modelling (SEM) will also be used in applied in this study to test the model.

Descriptive analysis will be the initial test to understand the respondent's feedback using frequency, mean and standard deviation. Factor analysis will be used to provide information on constructs' measurement reliability and validity. Following the aforementioned analysis, multiple linear regression will then be used to examine the relationship between independent and dependent variables. T-test and ANOVA will be used to understand the roles of demographics, in decisions affecting intention to use mobile payment devices. Structural Equation Modelling (SEM) will also be used to examine the measurement and structural fitness of the model [33]. These set of relationships, each with dependent and independent variables, will be the basis of SEM analysis.

## 10. Conclusion

Studies on security mechanisms focus on risks reduction by strengthening controls. Secure financial transactions based on adequate and robust controls are pertinent to the success of mobile payments. Consumers, however, do not fully understand mobile payment mechanisms and technologies. They can only perceive the strength of these security controls. It would be adequate for consumers to be sure that these controls exist and they perceive these controls, largely by way of awareness creation through advertising campaigns and publicity. The results of this survey would be critical, we hope, in validating the assertions this paper proposes on control mechanisms.

This paper highlights the importance of perceived security of mobile payments on consumer intention to use MP. We hope that the findings would encourage key players in the industries to create massive awareness campaigns towards informing potential consumers of the safety of their transactions. Social indicators like certification by a publicly tested control systems like SET protocols and other recognized certificate authorities is necessary in building MP trust levels. Trust seals like Web Trust and Trust-e would be important considerations. Apart from awareness through adverting schemes, they must ensure that all security mechanisms are robust enough to reduce the number of negative consumer experiences. Studies on increasing usability of new technologies have focused mainly on objective security. These studies are based largely on performance such as execution time and error rates. Most subjective studies focus on ease of use. In this paper, we hope to make recommendations to practitioners, based on the outcome of research data, on the need for subjective measures in assessing the effectiveness of security mechanisms. Mobile payment involves using wireless media, which is a precarious terrain. The key players should carefully assess trust issues as well as convenience in developing and advertising mobile payment schemes.

## 11. References

[1] K. Taga and J. Karlsson, *Arthur D. Little Global M-Payment Report*. Austria, Vienna, 2004.

[2] S. Karnouskos, "Mobile Payment: A journey through existing procedures & standardization initiatives " *IEEE Communications Surveys & Tutorials*, pp. 44-66, 2004.

[3] N. Mallat, "Exploring consumer adoption of mobile payments - A qualitative study," *Journal of Strategic Information Systems*, vol. 16, pp. 413-432, 2007.

[4] D. B. Begonha, A. Hoffman, and P. Melin, "M-payments; hang up, try again," *Credit Card Management*, vol. 15, pp. 40-44, 2002.

[5] Malaysian Communications and Multimedia Commission, *Q4 2007 Communications and Multimedia Selected Facts and Figures*. Cyberjaya: MCMC, 2008.

[6] Malaysian Communications and Multimedia Commission, *Hand Phone Users Survey '06*. Cyberjaya: MCMC, 2006.

[7] C. Shapiro and V. H. R, *Information Rules: A Strategic Guide to the Network Economy*. USA: Harvard Business School Press, 1999.

[8] J. Ondrus and Y. Pigneur, "Towards a holistic analysis of mobile payments: a multiple perspectives approach," *Electronic Commerce Research and Applications*, vol. 5, pp. 246-257, 2006.

[9] F. D. Davis, "Perceived usefulness, perceived ease of use, and consumer acceptance of information technology," *MIS Quarterly*, vol. 13, pp. 319-340, 1989.

[10] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behaviour*. USA: Prentice Hall, 1980.

[11] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behaviour," in *Action Control: From cognition to behaviour* J. Kuhl and J. Beckmann, Eds. USA: Springer, 1985, pp. 11 – 39.

[12] L. Chen, "A model of consumer acceptance of mobile payment',," *International Journal of Mobile Communications*, vol. 6, pp. 32-52, 2008.

[13] P. E. Pedersen, "Adoption of Mobile Internet Services: An exploratory study of mobile commerce early adopters," *Journal of Organisational Computing and Electronic Commerce*, vol. 15, pp. 203-222, 2005.

[14] W. Li and R. McQueen, "Barriers to mobile commerce adoption: an analysis framework for a country-level perspective," *International Journal of Mobile Communications*, vol. 6, pp. 231-257, 2008.

[15] B. Shneiderman, "Designing Trust into Online Experiences " *Communications of the ACM*, vol. 43, pp. 34-40, 2000.

[16] S. Chari, P. Kermani, S. Smith, and L. Tassiulas, "Security Issues in M-Commerce: A Usage-Based Taxonomy," in *E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand*, J. Liu and Y. Ye, Eds. Berlin: Springer, 2000, pp. 264-282.

[17] D. Khodawandi, K. Pousttchi, and D. G. Wiedemann, "Akzeptanz mobiler Bezahlverfahren in Deutschland," in *3rd Workshop Mobile Commerce*. Augsburg, Germany., 2003.

[18] F. Egger and D. Abrazhevich, "Security & Trust: Taking Care of the Human Factor," *Electronic Payment Systems Observatory Newsletter*, vol. 9, 2001.

[19] J. Ondrus and Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems," in *Sixth International Conference on the Management of Mobile Business (ICMB 2007)*, 2007.

[20] R. Bauer, "Consumer Behavior as Risk Taking " presented at 43rd National Conference of the American Marketing Association, 1990.

[21] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega*, vol. 28, pp. 725-737, 2000.

[22] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, pp. 709–734, 1995.

[23] D. H. McKnight and N. L. Chervany, "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology " *International Journal of Electronic Commerce*, vol. 6, pp. 35–59, 2001.

[24] M. Merz, *E-Commerce and E-Business: Marktmodelle, Anwendungen und Technologien.*, 2nd ed. Heidelberg: Dpunkt Verlag, 2002.

[25] Litan et al., "Understanding and Preventing Data Compromises Maintaining Trust in Payments:," in *A Security Summit* Washington, DC, 2007.

[26] A. Bhimani, "Securing the Commercial Internet " *Communications of the ACM*, vol. 39, pp. 29-35, 1996.

[27] S. Ganesan, "Determinants of long-term orientation in buyer-seller relationships," *Journal of Marketing*, vol. 58, pp. 1-19, 1994.

[28] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Empirical Models," *Management Science*, vol. 35, pp. 982–1003, 1989.

[29] E. Babbie, *Survey Research Methods*. Belmont: Wadsworth, 1990.

[30] U. Sekaran, *Research Methods for Business: A Skill-Building Approach*, 2nd ed. New Jersey: John Wiley & Sons, 2003.

[31] D. Compeau, "Computer Self-efficacy: Development of a Measure and Initial Test," *MIS Quarterly*, vol. 19, pp. 189-211, 1995.

[32] J. S. Armstrong and T. Overton, "Estimating non-response bias in mail surveys," *Journal of Marketing Research*, vol. 14, pp. 396-402, 1977.

[33] C. Dewberry, *Statistical methods for organizational research: theory and practice*. New York: Routledge, 2004.