Asian Journal of Business Management 4(3): 275-285, 2012
ISSN:2041-8752

Submitted: March 14, 2011 Accepted: March 26, 2012 Published: June 25, 2012

Survey of Customers' Conceptions of Security and Trust in E-Payment System

[1]Fakhraddin Maroofi, [2]Reza Hashemi and [3]Zohre Nargesi
[1]Kurdistan University, Iran
[2]Razi University, Iran
[3]Islamic Azad University, Kermanshah Branch, Iran

Abstract: In this study, we examine issues related to e-payment security from the viewpoint of customers. This study proposes a conceptual model that delineates the determinants of consumers' observed security and observed trust, as well as the effects of observed security and observed trust on the use of e-payment systems. To test the model, structural equation modeling is employed to analyze data collected from 219 respondents in Iran. This research provides a theoretical foundation for academics and also practical guidelines for service providers in dealing with the security characteristic of e-payment systems.

Keywords: E-Payment Systems (EPS), electronic commerce, EPS use, security, trust

INTRODUCTION

Electronic Commerce (EC) is built upon E-Payment Systems (EPS). As EC becomes a major element of business operations for many companies, e-payment has become one of the most scathingissues for successful business and financial services (Linck *et al*., 2006; Cotteleer *et al*., 2007; Kousaridas *et al*., 2008). In comparison to the traditional payment methods, e-paymenttechniques have favorable characteristics, including security, reliability, acceptability, isolation, efficiency and advantage (Tsiakis and Sthephanides, 2005; Linck *et al*., 2006; Cotteleer *et al*., 2007; Kousaridas *et al*., 2008). E-Payment Systems (EPS) have obtained recognition and have been positioned throughout the world. In this research we use empirical investigation in Iran because the supporting infrastructure need for the EPS development has been put in place. Iran has confrontationally followed the development of IT and networks. Since the mid-2001s, the Iran government has enforced a number of policies for spreading and promoting EC. The e-commerce market in Iran is expected to double annually in the next five years. A key factor for the success of EPS is security, a need that is becoming even more critical in the current global EC environment (Herzberg, 2003; Stroborn *et al*., 2004; Linck *et al*., 2006; Cotteleer *et al*., 2007). Arrangements in EC can occur without any preceding human contactor create interpersonal relationships. EC security threats from the interpersonal networks can trust in EPS and cause people to fall back on the interpersonal trust that arises in human-to-human interactions. Generally, security is a set of procedures, mechanisms and computer programs for proving the source of information and guaranteeing the process (Linck *et al*., 2006). (Linck *et al*., 2006) stated that technical details of security and trust in EPS from the perspective of company or EPS service providers, consumers' conceptions of the security of EPS have not been well presented and empirical studies are lacking in this area. Although various security measures and mechanisms have been designed for these EPS, but still problems are remain (Hsieh, 2001; Dai and Grundy, 2007; Kousaridas *et al*., 2008). Hence, there is a need to minimize the risks related with e-payment arrangement processes (Tsiakis and Sthephanides, 2005). Since the majority of users of EPS are relatively unfamiliar with the technical details of EPS, they tend to evaluate the security level of EPS on the basis of their experience with user-interfaces. Thus, to attract and keep e-payment users, it is essential to increase consumers' conceptions of security and to maintain customers' trust during e-payment arrangements (Chellappa and Pavlou, 2002; Linck *et al*., 2006, Kousaridas *et al*., 2008). The principal objective of this research is to empirically examine, from the view point of consumers, the resolves is that affect consumers' conceptions of security and trust, as well as the effects of observed security and observed trust on the use of EPS.

THEORETICAL BACKGROUND

When EC created the need for e-payment services, traditional cash-based and account-based payment instruments were used as a model. E-Payment is defined as the transfer of an electronic value of payment from a payer to a payee through an e-payment mechanism. E-Payment services exist as web-based user-interfaces that allow customers to withdrawn access and manage their bank accounts and arrangements (Weir *et al*., 2006; Lim,

Corresponding Author: Fakhraddin Maroofi, Kurdistan University, Iran

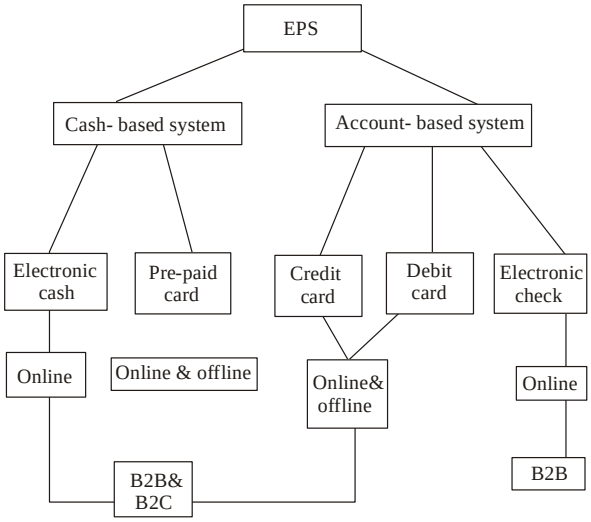

Fig. 1: Classification of electronic payment systems

2008). In general, EPS can be classified into five categories (Lawrence *et al*., 2002; Abrazhevich 2004; Dai and Grundy, 2007; Schneider, 2007), such as:

- Pre-paid card
- Electronic-cash
- Debit cards
- Credit cards
- Electronic checks

Electronic-cash, pre-paid cards, credit cards and debit cards are widely used in B2C and C2C EC (Theodosios and George, 2005), as shown in Fig. 1. This study focuses on these four types of EPS. Pre-paid cards are issued for a specific value by a particular company and are regularly used in store arrangements. The card can be given as a gift or just used as a suitable way of making purchases. The pre-paid card is favorable for companies because customers tend to spend more freely when using it Kniberg (2002). Debit card is one of the most considerable used systems for e-payment. The debit card procedure combines the characteristic of the Automatic Teller Machine (ATM) card with Internet banking. When customers pay with a debit card, money is automatically deducted from their bank accounts. In contrast with credit cards, the expended money comes directly from a bank account. Many banks issue a debit card that can be used in places where credit cards are not accepted. When users pay with a debit card, the payment is processed as a debit arrangement (Abrazhevich, 2004). Electronic cash is a procedure of payment in which a special recognition number is related with a specific amount of money. Electronic cash is referred to as e-cash (Jewson, 2001; Wright, 2002; Chou *et al*., 2004). This method was developed as asubstitute to the use of credit cards for Internet purchases of goods or services. For using this payment system, customers purchase electronic digital-cash from the issuing company (Abrazhevich 2004). The cash may be transferred through computers or other telecommunications channels (Hsieh, 2001). The digital-cash method needs a single organization for the issuance and saving of cash. The low cost characteristic of electronic cash makes it one of the most encouraging methods for micro-payment (Lawrence *et al*., 2002; Kim *et al*., 2006). Credit card payments arise from offline credit card mechanisms (Lawrence *et al*., 2002). Credit cards are the most regularly used form of e-payment. Two important issues related with the credit card (Hsieh, 2001; Chou *et al*., 2004) method are security (Stroborn *et al*., 2004) and isolation, since consumers' arrangement records can be tracked through their credit cards (Laudon and Traver, 2001). The credit card method involves an irreducibly complex arrangement-structure (Hsieh, 2001; Wright, 2002). Compared to other EPS, it is not suitable for small-value arrangements (Kalakota and Whinston, 1996).

Pre-paid cards, credit cards and debit cards are the most regularly employed e-payment procedures in B2C and C2C EC, whereas the electronic-cash procedure operates as a supplement to them. Each e-payment technique performs an important function in EC arrangements. The electronic-cash procedure issuitable for small-value arrangements while the pre-paid cards, credit cards and debit cards can be employed for most types of arrangement, although small-value arrangements can be disportionately costly. Since no single e-payment system clearly principal in EC arrangements, each e-payment

system can operate as a supplement to the others. Security issues are also of involve for small-value e-payment arrangements. For large-value arrangements, security is the most critical issue and the use of other security mechanisms should be accordingly considered in order to reduce e-payment arrangement risks.

Analysis of the literature: In order to identify the factors that affects consumers' observed security and observed trust in the use of EPS in B2C and C2C EC, this section analysis the applicable literature and provides a conceptual foundation. Since the Internet is an open network with no direct human control over individual arrangements, the technical infrastructure that supports EC and EPS must beun affected to security attacks. Technical defended that are design to reduce this kind of risk need to be taken into consideration before the problem of consumer trust is presented. Kalakota and Whinston (1997) evaluate some of the issues related with the security of EPS. They note that EPS should be thickened profit security infringements and that the unprotected of EPS should be carefully considered. The security of e-payment arrangements depends on a number of factors, such as systems factors, i.e., technical infrastructure and implementation (Laudon and Traver, 2001; Linck *et al*., 2006), arrangement factors, i.e., secure payment in accordance with well-defined rules (Hwang *et al*., 2007; Lim, 2008) and legal factors, i.e., a legal framework for electronic arrangements (Peha and Khamitov, 2004). Analyzing present security technologies for EPS, including encryption and confirmation techniques, Slyke and Belanger (2003) suggest that a secure e-payment system should provide security aprofittcheating activities and must protect the isolation of consumers. Finally, Romdhane (2005) stated the importance of security evaluation for EPS and argues that a secure e-payment system must show the following two elements:

- Integrity, which contains confirmation, fraud prevention and isolation
- Divisibility, transferability, duplicate spending prevention, payment certainly and payer discoverable

The procedures in e-payment solutions differ from the ones in the traditional payment solutions because the arrangement infrastructures are basically different from each other; this may engender a range of new security issues, including pertain to over unauthorized use and arrangement level (Linck *et al*., 2006; Hwang *et al*., 2007; Lim, 2008). Although an e-payment system has the advantage of overcoming time and space limitation when compared to the traditional offline arrangements, consumers' conceptions of security and the trust they place in systems are of important for increasing the use of these systems (Linck *et al*., 2006; Kousaridas *et al*., 2008). Laudon and Traver (2001) suggest that sophisticated procedures and process interactions should be developed in EPS to deal with security need. Lawrence *et al*. (2002) suggest that processed process interactions in EPS can remove consumers' anxieties over security issues related with the use of EPS. Supporting security declaration in e-payment sites is another important step (Mukherjee and Nath, 2003; Cotteleer *et al*., 2007; Lim, 2008); the term, ''security declaration", refers to the information assuming that to consumers for EPS operations and security solutions. However, few studies show the importance of security declaration in EPS. Miyazaki and Fernandez (2000) suggest that security-related declarations that are supported on websites are likely to increase the chances of consumers' purchasing and paying over the Internet. The realistic supporting this proposal has its basis in the concept of information asymmetry and the role that it plays in decision-making. Information asymmetry refers to circumstances in which one of the parties connected in aarrangement does not have approach to all the information needed for decision-making (Akerlof, 1970). This has been recognized as one of the major problems in EPS. According to Mukherjee and Nath (2003), the extent of information asymmetry should influence customer's conceptions of security and trust in EPS. Friedman *et al*. (2002) also suggest that the declarations of security characteristic declaration of data defense and isolation, security-policy declarations and other descriptive satisfied pertaining to security insurance help users construct more correct explanations of what a secure e-payment system means. Consumers are exceptionally responsive to the risks connected in personal and isolation information security. A great deal of preceding empirical research has focused on the technical details of defense, such as isolation and integrity, which are unfavorable for consumers' use of EPS (Linck *et al*., 2006; Hwang *et al*., 2007; Kousaridas *et al*., 2008). However, arrangement procedures for confirmation and modification are also important in EPS (Linck *et al*., 2006; Hwang *et al*., 2007; Kousaridas *et al*.,2008). The availability and comprehensibility of security declaration are also important for e-payment

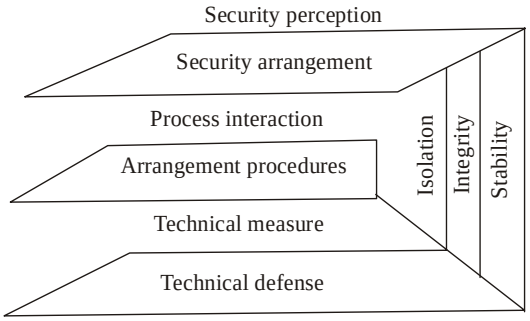

Fig. 2: Diagram of factors that influence observed security and observed trust in EPS use

arrangements(Cotteleer *et al*., 2007; Lim, 2008). All three of these dimensions should be considered in the design of secure EPS. Based on this analysis of the literature, we can classify the factors that influence consumers' conceptions of security and trust in the use of EPS into three areas: security declarations; arrangement procedures; and technical contribution (Fig. 2). As described earlier, security declaration refers to the information assuming that to consumers in relation with EPS operation and security solutions. Technical contribution refers to technical mechanisms to protect consumers' arrangement security. Arrangement procedures refer to the steps that are designed to facilitate the actions of consumers and remove their security anxieties.

RESEARCH MODEL AND HYPOTHESES

There is little research on the direct relationship between consumers' observed security and observed trust in EPS. A notable exception is the study of Chellappa and Pavlou (2002). They conclude that online arrangements are subject to multiple security threats and propose that consumers' trust in online arrangements is influenced by their observed security. They test this proposal and demonstrate a significant, positive relationship between consumers' conceptions of the security of online arrangements and their trust in these arrangements. Theodosios and George (2005) state that e-payment service providers must take into account trust and security as important characters of consumers' use of EPS. Top resented this issue, we develop a examine questionnaire by adopting the security study framework proposed by Linck *et al*. (2006). They focus on the security issues influencing customers' contribution in a mobile payment procedure and classify the security conception into two dimensions: objective security and subjective security. This research cadges their idea of objective and subjective security dimensions. In the objective dimension, we regard security measures as the definite solutions in EPS that respond to all security concerns, including technical contribution, arrangement procedures and security declaration. However, average customers find it difficult to objectively estimate the security solutions of EPS (Egger and Abrazhevich, 2001); most of them estimate the security of EPS based on their current interface with the system. Consumers' subjective evaluations of security have no effect on objective security measures, whereas the level of objective security measures influences consumers' subjective evaluations of security (Linck *et al*., 2006). This study tests a research model of consumers' EPS use, which is influenced by both consumers' conceptions of security and trust. We integrate consumers' observed security and observed trust into the research model by assuming that both security and trust are important pertain for consumers during an e-payment arrangement. If an e-payment system does not sufficiently provide a secure arrangement environment, consumers will treat the system with feeling, which may undermine consumers' trust and finally their use of the system (Mukherjee and Nath, 2003; Linck *et al*., 2006; Kousaridas *et al*., 2008). Figure 3 summarizes our research model, based on the research hypotheses developed. While some of the EPS security factors identified in this model have been presented in previous studies, our research model identifies new antecedents that are considered important to consumers' conceptions of security and trust, in addition to incorporating both observed security and observed trust. As shown in the model, technical contribution, arrangement procedures and security declaration are the principal factors for consumers' conceptions of security and trust in the utilization of EPS. These three factors are directly responsible for determining whether or not a consumer would consider an e-payment system to be secure and whether or not a consumer would have trust in EPS.

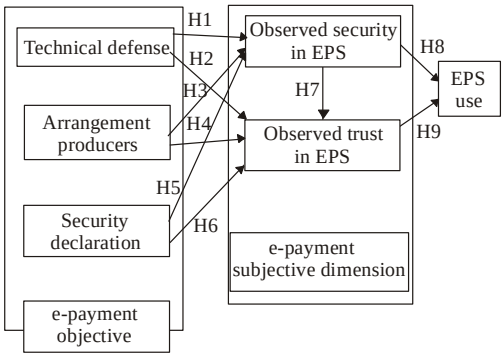

Fig. 3: The model of observed security and observed trust in EPS use

Research hypotheses: Technical contribution is considered to be the substructure of EPS security. In relation with this conception, Chellappa and Pavlou (2002) assert that observed security and observed trust will be favorably influenced by technical contribution, including isolation, integrity and stability. If an e-payment system can off era guarantee regarding isolation, integrity and stability, then the level of consumers' observed security and observed trust in EPS can be increase (Tsiakis and Sthephanides, 2005; Hwang *et al*., 2007). Accordingly, we hypothesize that technical contribution are likely to utilize a positive impact on consumers' conceptions of both security and trust:

H1: Technical securities are positively related with consumers' observed security in EPS.

H2: Technical securities are positively related with consumers' observed trust in EPS.

The main objective of arrangement procedures is to promote consumers' use of EPS and to remove their concerns about the security of EPS (Lawrence *et al*., 2002). To achieve consumers' security needs, well-defined EPS procedures should be prepared (Hwang *et al*., 2007). Therefore, three principal procedures are deployed during the arrangement process:

- Confirmation each contributor preceding to the arrangement
- Providing consumers toward the entire of the e-payment arrangement
- Sending an acknowledgement after each arrangement to satisfy consumers that the e-payment system has successfully carry out the task (Tsiakis and Sthephanides, 2005; Hwang *et al*., 2007).

We hypothesize that arrangement procedure sutilize a positive effect on both observed security and observed trust in EPS:

H3: Arrangement procedures are positively related with consumers' observed security in EPS.
H4: Arrangement procedures are positively related with consumers' observed trust in EPS.

By informing consumers regarding the security of their payment options, it will be possible to influence consumers' conceptions of security and trust in EPS (Lim, 2008). If normal consumers remain unaware of the level of security that is basic to their arrangements, they will be opposed to engage in e-payments (Hegarty *et al*., 2003; Lim, 2008). Consumers' decisions to use any e-payment system will be considerably influenced by the quality of security declarations available to them. This idea is supported by the results reported by Miyazaki and Fernandez (2000), as stated earlier, argue that security-related arrangement that are shafted on websites are likely to increase the chances of consumer purchase over the Internet. We hypothesize that security arrangement utilize a positive effect on both consumers' observed security and observed trust in EPS:

H5: Security arrangement is positively related with consumers' observed security in EPS.
H6: Security arrangement is positively related with consumers' observed trust in EPS.

Observed security refers to the customer's subjective evaluation of the e-payment system's security (Linck *et al*., 2006). Since consumers own different experiences and expectations, they may adopt different perspective towards the security of online arrangement. This is true even if e-payment systems provide guarantee with regard to all characteristic of consumer's security needs (Stroborn *et al*., 2004). If the level of observed security in an e-payment arrangement is too low, consumers are unlikely to share in the arrangement until solutions are implemented to decrease their anxieties (Tsiakis and Sthephanides, 2005). Security and trust worthiness are the main concerns for customers who use EPS and they are related to each other (Linck *et al*., 2006). Thus, we propose two hypotheses regarding the role of observed security in relation to consumer's observed trust and EPS use:

H7: Observed security in EPS is positively related with consumers' observed trust in EPS.
H8: Observed security in EPS is positively related with consumers' use of EPS.

Consumers can make a realistic decision based on the knowledge of possible rewards for trusting and not trusting. Trust enables higher profit while distrust avoids potential losses (Linck *et al*., 2006; Kousaridas *et al*., 2008). Consumers' perspectives toward EPS are contribution with their conceptions of the systems' security. Consumers' observed trust in EPS is defined as consumers' belief that e-payment arrangement will be processed in accordance with their expectations (Tsiakis and Sthephanides, 2005; Mallat, 2007). Kniberg (2002) stated that ''users and company are more likely to use an insecure payment system from a trusted company than a secure payment system from an un trusted company (p. 60)". This is constant with the findings of the previous studies (Tsiakis and Sthephanides, 2005; Mallat, 2007), which suggest that trust is more important than security. Without customer trust, it would be exceptionally difficult for an EPS to achieve worldwide usage. Thus, wehypo the size that consumers' observed trust in EPS influences the use of EPS:

H9: Observed trust in EPS is positively contribution with consumers' use of EPS.

Measurement: This research measures technical contribution by using the following three categories: integrity; sensitively and isolation (Friedman *et al*., 2002; Tsiakis and Sthephanides, 2005; Hwang *et al*., 2007). Integrity measures the security of payment information both during and after a payment process (Romdhane, 2005). Integrity mechanisms confirm that other parties do not change e-payment information (Hwang *et al*., 2007; Kousaridas *et al*., 2008). Consumer's need that the integrity of e-payment information is confirms and that the amount of payment and other data remain unchanged (Laudon and Traver, 2001). This mechanism influences consumers' conceptions of security and trust in EPS use.

Sensitively refers to the prevention of unauthorized parties from capturing, explaining, or understanding data. Sensitively performs a critical function in gaining consumers' belief in EPS. There are a variety of factors that may affect the sensitively of electronic arrangements, including e-payment software, e-payment databases, e-payment system platforms and power supply (Kalakota and Whinston, 1997). Additionally, technical defense of establishing confirmation of parties, such as the two-factor confirmation, is also important for sensitively. Finally, an isolation-defense mechanism can satisfy consumers that their personal information, such as names, addresses and contact details, will not be released to other parties (Wright, 2002; Peha and Khamitov, 2004). Consumers would like to confirm that the information assuming that to company during an e-payment process cannot be used by other parties (Slyke and Belanger, 2003; Chou *et al*., 2004). These technical contributions can be achieved by certain policies, including standardization as to the way in which consumers' information is utilized, stored and securely defend (Pilioura, 2001). Some consumers are opposed to use EPS, simply because they anxiety that their personal details can be misused on the Internet (Kalakota and Whinston, 1997; Wright, 2002). The use of two different factors as opposed to one factor delivers a higher level of confirmation guarantee (Friedman *et al*., 2002; Tsiakis and Sthephanides, 2005). This research measures arrangement procedures by using the following three factors: confirmation; modification; and confirmation. Confirmation is the procedure by which the character of contributors is verified through their character and password before they share in an e-payment system (Tsiakis and Sthephanides, 2005; Hwang *et al*., 2007). Although confirmation offers a primary procedure for stopping illegal intrusions, it is subject to a number of risks that arise from the open nature of the Internet. Confirmation is a visible procedure that is directly related to payment security and thus influences consumers' conceptions of security and trust (Tsiakis and Sthephanides, 2005; Kousaridas *et al*., 2008). Modification is the procedure by which consumers modify their payment amount or method preceding to the completion of the final stage of the payment process. The supply of such an option can also give consumers a conception of belief and regurantee that they have control over their payment arrangements until the finalization stage (Laudon and Traver, 2001). Confirmation is the procedure by which consumers can be satisfied that their payments have been received by company (Linck *et al*., 2006). In this procedure, company send an acknowledgement by using mobile phone messages, emails, faxes, etc. The supply of acknowledgement information regarding a payment affects consumers' conceptions of security and trust in EPS use Romdhane (2005).

This research measures security declarations through three factors: accessibility; availability and comprehensibility. First, accessibility refers to the advantage with which consumers can locate declaration that concern the security characteristic of EPS (Wright, 2002; Hegarty *et al*., 2003). Consumers should not need to utilize any special or extraordinary efforts to locate security declaration. They should be made available either on the e-payment webpage or on other linked web pages. Thus, a well-designed e-payment system should make it relatively easy for customers to locate security declaration (Cotteleer *et al*., 2007). Second, availability refers to the information that supports consumers' use of an e-payment system (Mukherjee and Nath, 2003). Consumers need knowledge regarding what options and functions are assuming that by EPS. Insufficient declaration can be an obstacle to consumers' use of EPS (Lim, 2008). Therefore, a well-designed e-payment system should provide declaration concerning the technical description and functionality of EPS, namely:

- Functions and options within an e-payment
- Explanations as to how to use an e-payment function
- Advice on how to prevent defaults on an e-payment system (Miyazaki and Fernandez, 2000; Tsiakis and Sthephanides, 2005; Lim, 2008)

In addition to information that allows customers to distinguish between trustworthy and non-trustworthy company, other information could also be assuming that by EPS.

Finally, comprehensibility refers to the way in which security declaration is assuming that to the consumers (Linck *et al*., 2006). The security declaration should be clear and simple enough for an average consumer to understand easily. They should also attract consumers' attention when customers make an e-payment arrangement (Mukherjee and Nath, 2003). Therefore, a well-designed e-payment system should have the following characteristics:

- The declaration should be comprehensive and clear
- The declaration should attract consumers' attention (Hsieh, 2001; Cotteleer *et al*., 2007)

METHODOLOGY, DATA ANALYSIS AND RESULTS

Measurement evaluation is used to validate our model. Following recommendations of preceding studies for developing and validating measurement instruments (Hair *et al*., 2003; Novak *et al*., 2000), our study conducts a three-stage procedure. The first stage is a set of sample items to produce for each construct and evaluated for the

reliability and satisfied validity (Joreskog and Sorbom, 1993; Kline, 1998).The second stage, is running through an analysis of the applicable literature and corresponding scales (Gefen *et al*., 2000). In the third stage, we proceed with a considerable confirmatory analysis for EPS by testing and validating the processed scales for the reliability and construct validity. We verify convergent validity and the goodness-of-fit of our research model. This research uses Iran as the site of the empirical investigation. This research carried out a two-stage, first, proceeding to the conduct of a formal study, a pretest was carried out to validate the primary report of the questionnaire. The samples for the pretest were obtained from the university located in Iran. The sample consist 30 undergraduates and graduate students, all of them had no specific technical background in EPS, but had used EPS before. Two IS teachers were asked to analysis the questions to improve the construct validity. Therefore each questionnaire item was scored on a four-point Likert scale (1 = strongly disagree; and 4 = strongly agree). The questionnaire contained a few nominally scaled background questions. A structured, paper-based questionnaire was used in a formal study, which was running to evaluate the proposed model and to validate the proposed set of interrelationships that were contribution with consumers' conceptions of security and trust in the use of EPS. The study was running with contributors on a large scale of a 35-item questionnaire. The questionnaire has six sections: technical contribution, arrangement contribution, security declaration, observed security in EPS, observed trust in EPS and EPS use. A total of 960 questionnaires were distributed in 2010. The questionnaires were distributed through the mail, personal visits and email to people who were working in different industries and social institutions, including universities, offices, research institutes and companies that were drawn at random in Iran. To process the measures and to evaluate their reliability and validity, the study was running with guidelines. Each contributor was carefully complete the questionnaire and directed to evaluate the degree of their faith in technical contribution, arrangement procedures, security declaration, observed security, observed trust and EPS use, which they would expect from a prospective e-payment with particular online company. Altogether, 275 questionnaires were collected by mail, personal visits and email. 34 questionnaires were removed due to invalid answers or a lack of experience in the use of EPS, leaving 241 questionnaires for our empirical analysis (a response rate of 23.1%). Our sample consisted 65.4% male and 34.6% female respondents. Most respondents were experienced users of EPS. In terms of age, 15.2% of contributors were between 16 and 25 years, 50.9% between 25 and 35 years, 23.8% between 36 and 45 years and 10.1% older than 45 years. However, young and middle-aged users of EPS represent a significant portion of the user population in Iran. According to Lin and Lu (2000), the results obtained from the analysis of this type of sample can still reflect true phenomena and provide significant results because young and middle-aged users are the most important of the user population and because, these users will be the most active consumers in EC in the future. Thus, the sample can be considered as being representative of the whole population of users of EPS in Iran.

Table 1: KMO value and Bartlett's test

Kaiser-Meyer-Olkin measure of sampling adequacy		0.866
Bartlett's test of sphericity	Approximate Chi-square	3572.301
	Degrees of freedom	406
	Significance	0.000

Validity test: Factor analysis identifies the essential structure within a set of observed variables (Miyazaki and Fernandez, 2000). SPSS software was used in the evaluation of validity. We evaluated the construct validity by identifying the conceptions of observed security and observed trust. In addition, factor scores were derived from the identified elements from the formal study questionnaire. An exploratory factor analysis is primarily running with rotations to recognize the significance of the hypothesized factors (convergence validity). All Eigen values are set to greater than one and the items are reduced to their principal constructs. Finally, a principal element analysis is used as the extraction method for confirmatory factor analysis with varimax rotation. Twenty-nine study items in the questionnaire were applicable to factor analysis. To determine the essential structure, the correlation matrix was primarily examined to determine how suitable it was for factor analysis. The KMO (Kaiser-Meyer-Olkin) values for each of the 29 study items go bounded 0.45. In addition, the value of the test statistic for on the basis of a Chi-squared transformation of the determinant of the correlation matrix was large (0.866) and the contribution significance level was exceptionally small (0.000). As shown in Table 1, we concluded that the data were multivariate normal data. Furthermore, the correlation matrix contained sufficient co-variation for factoring. To determine that technical contribution, arrangement procedures, security declaration, observed security, observed trust and EPS use are separate variables, a confirmatory factor analysis was running through SPSS. The primary element solution was rotated by using the varimax procedure, with elements whose Eigen values were greater than one, which is the criterion for factor retention. Based on the Screen test and the Eigen values that were greater than one, five factors were accepted as interpretable factors. These factors accounted for 62.01% of the variance. Table 2 shows the results of our factor analysis.

Table 2: Rotated component matrix

	Component					
Items	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	
TECH4	0.795					
TECH5	0.721					
TECH2	0.695					
TECH1	0.642					
TECH3	0.564					
PROC4		0.812				
PROC5		0.755				
PROC3		0.670				
PROC2		0.643				
PROC1		0.617				
TRUS3			0.787			
TRUS2			0.724			
TRUS1			0.671			
SECU2				0.734		
SECU1				0.694		
SECU3				0.603		
USE2					0.807	
USE1					0.805	
USE3					0.793	
DECL1						0.777
DECL2						0.732
DECL4						0.675
DECL3						0.592
Eigen values	3.550	3.324	3.103	2.887	2.342	2.190
% of variance	12.240	11.463	10.699	9.955	8.077	7.573
Cumulative %	12.240	23.703	34.402	44.357	52.434	60.003

Table 3: Reliability coefficient test

Scales	Number of items	Alpha	Mean	Standard deviation
Technical defense	5	0.8399	4.24	0.62
Arrangement procedures	5	0.8144	4.17	0.40
Observed security	3	0.7489	4.18	0.44
Observed trust	3	0.8902	4.21	0.60
EPS use	3	0.7707	4.11	0.41

n: 241

Table 4: Indices of fit and comments for model analysis

Indices in SEM analysis	Default model	Data fitting of the model
Chi-square/degrees of freedom ratio	686.546/368 = 1.865	Good fit (should < 3)
RMR (root mean square residual)	0.079	Good fit (should < 0.08)
GFI (goodness of fit index)	0.868	Not a good fit (should > 0.90)
AGFI (adjusted GFI)	0.830	Good fit (should > 0.80)
NFI (normed fit index)	0.805	Not a good fit (should be > 0.90)
RFI (relative fit index)	0.791	Not a good fit (should be > 0.90)
IFI (incremental fit index)	0.906	Good fit (should be> 0.90)
CFI (comparative fit index)	0.901	Good fit (should be > 0.90)
RMSEA (room mean square error approximation)	0.065	Good fit (should be < 0.08)

Reliability test: Reliability is determined by Cronbach's alpha, for measuring reliability (Mukherjee and Nath, 2003). Nunnally (1978) suggests that for any research at its early stage, a reliability score or alpha that is 0.60 or above is sufficient. Table 3, show the reliability scores of all the constructs were found to go beyond the beginning set by Nunnally; all measures demonstrated good levels of reliability (greater than 0.72). The observed trust scale achieved the largest reliability of 0.8932. As suggested in the literature (Joreskog and Sorbom, 1993; Kline, 1998), the model fit is evaluated by such indices as the Comparative Fit Index (CFI), the Goodness of Fit Index (GFI; Hair *et al*., 2003), the Normed Fit Index (NFI) and the Root Mean Square Error of Approximation (RMSEA; Steiger, 1990). The Comparative Fit Index is an index of overall fit (Gerbing *et al*., 1993). The Goodness of Fit Index measures the fit of a model compared to other models (Hair *et al*., 2003). The Normed Fit Index measures the portion by which a model is improved in terms of the fit, when compared to the base model (Hair *et al*., 2003). The RMSEA provides information in terms of the difference for the degrees of freedom for a model (Steiger, 1990). The accepted beginnings for GFI, RFI, NFI and CFI are 0.90; RMSEA is recommended to be at

Table 5: Hypotheses-testing of the research model

Hypothesized path	Estimate	SE	T	p-value
Arrangement procedures? observed security in EPS	−0.065	0.040	−1.629	0.105
Technical protections? observed security in EPS	0.357	0.050	7.049	0.000**
Arrangement defense? observed trust in EPS	0.075	0.061	1.176	0.231
Technical defense? observed trust in EPS	0.398	0.081	4.961	0.000**
Perceived security in EPS? observed trust in EPS	0.412	0.139	3.015	0.003**
Observed security in EPS? EPS use	0.271	0.150	1.809	0.010*
observed trust in EPS?EPS use	0.288	0.076	3.829	0.000**

*: $p<0.05$; **: $p<0.01$

most 0.06 and acceptable up to 0.08 (Gefen *et al*., 2000). The correctness of the research model was tested by using structural equation modeling techniques with AMOS 6.0. The Chi-square statistic of the model was 685.436 with 359 of freedom, thus showing a good fit with the model (a ratio of less than 3). However, since the Chi-square test is very sensitive to the sample size, we employed a number of other indices to further test the model fit. As shown in Table 4, all the indices-RMR, GFI, AGFI, CFI, NFI, RFI, IFI and RMSEA are at acceptable levels. Overall, the results showed that our model provides a valid framework for the measurement of consumers' observed security and observed trust in EPS.

In this section we present the statistical results of the measurement validation and hypothesis testing. The effects of technical contribution, arrangement contribution and security declaration on consumers' conceptions of security and trust in EPS were evaluated through AMOS 6.0 (Table 5).Table 5 shows that the effects of technical contribution and security declaration on consumers' observed security in EPS were significant (βTECH = 0.358, t = 7.049, $p<0.01$ and βSTAT = 0.251, t = 2.814, $p<0.01$).3 Hence, Hypothesis 1 (H1) and Hypothesis 5 (H5) are strongly supported by the results. In contrast, the effect of arrangement procedures on consumers' observed security was not significant (βPROC = -0.065, t = -1.629, p = 0.105), showing that arrangement procedures do not act as an antecedent of consumers' observed security in EPS. Hence, Hypothesis 3 (H3) is not supported. Our results show that technical contribution (βTECH = 0.398, t = 4.961, $p<0.01$) and observed security in EPS (βSECU = 0.412, t = 3.015, $p<0.01$) are strongly contribution with consumers' observed trust in EPS. Thus, Hypothesis 2 (H2) and Hypothesis 7 (H7) are supported. On the other hand, the effects of security declaration (βSTAT = 0.154, t = 1.239, p = 0.215) and arrangement procedures on consumers' observed trust (βPROC = 0.075, t = 1.176, p = 0.231) were not significant; thus, Hypothesis 4 (H4) and Hypothesis 6 (H6) are not supported. Our results also show that consumers' observed trust in EPS utilize a substantial effect on consumers' EPS use (βTRUS = 0.288, t = 3.829, $p<0.01$), thus validating Hypothesis 9 (H9). Finally, the impact of consumers' observed security in EPS is positively contribution (βSECU = 0.271, t = 1.809, $p<0.05$) with consumers' EPS use, thus supporting Hypothesis 8 (H8). Overall, the path coefficients of H1, H2, H5, H7 and H9 were significant at a level of $p<0.01$, thereby showing support for these hypotheses. The path coefficient of H8 was significant at a level of $p<0.05$, thus showing support for the eighth hypothesis. Hypotheses 3, 4 and 6 are not supported. Figure 4 shows a summary of our results for each hypothesis in the research model. The significance of the estimates is shown by a solid line. Consumers' observed security in EPS use is determined by technical contribution and security declaration. It is also clear that observed security and observed trust are significant factors that influence consumers' EPS use. Additionally, there is a significant impact of observed security on observed trust.

CONCLUSION AND IMPLICATIONS

Our research proposes a research model that delineates the determinants of consumers' observed security and observed trust, as well as the effects of observed security and observed trust on EPS use. Our findings show that both technical contribution and security declaration are significant factors for improving consumers' observed security. Consumers' observed security is positively related to consumers' observed trust and EPS use. Finally, consumers' observed trust also has a positive impact on EPS use (Culnan and Armstrong, 1999; Miyazaki and Fernandez, 2000). This study provides important theoretical and practical contributions to the area of security and trust in EPS. This research develops a theoretical model of consumers' observed security and observed trust, including their roles in the use of EPS. It helps to explain the direct relationships between observed security, observed trust and EPS use. Our results clearly delineate the role of consumers' observed security in building the trust of consumers and the positive impact of both observed security and observed trust on EPS use. The effects of both technical contribution and security declaration on consumers' conceptions of security and trust are also validated. Consumers' observed security and observed trust are essential conceptions in our understanding of consumers' use of EPS. This research is consistent with previous claims that both observed security and observed trust perform a critical function in promoting consumers' EPS use. By presenting an empirically devised set of security issues in EPS in B2C and C2C EC, this research can serve

as a basis for the selection of suitable indicators for further empirical research. This study suggests that mere introduction of e-payment services is not going to be sufficient to attract consumers to B2C and C2C EC. E-Payment service providers should decrease the security concerns of consumers and promote customers' belief in the trustworthiness of services. Some e-payment service providers merely concentrate on technical contribution and ignore the importance of security declaration in the system. Others hold the idea of ''more is better" or ''as detailed as possible" on procedural design, based on the objective dimension of security, which seems to be reasonable in terms of obtaining consumers' belief in EPS. However, from the subjective viewpoint of consumers, this practice ignores the simplicity of use in operation and thus, can be counterproductive. It is importance for e-payment service providers to develop systems that are deemed as secure on both objective and subjective levels. Thus, management needs to focus on the promotion of these beliefs among consumers when designing security systems. This study finds no evidence of a statistically significant relationship between the quality of arrangement procedures and consumers' observed security or observed trust in EPS use. The magnitudes of the estimates are quite small and thus do not support Hypothesis 3 (H3) and Hypothesis 4 (H4). These results are not consistent with the results of the study running by Laudon and Traver (2001) and Romdhane (2005). One possible explanation is that complex procedures, such as fussy confirmation and log-in procedures erode consumers' advantage in using certain e-payment systems. The advantage consumers experience in the arrangement procedures might degrade consumers' valuation of the security and the trustworthiness of the e-payment system. Thus, e-payment service providers may have to provide consumers with not only secure procedure but also convenient procedures for e-payment systems. This study is not free from limitations. First, the sample employed for our empirical analysis was collected from Iranian consumers. The issues contributions with e-payment are widely recognized in countries with more advanced EC settings. Thus, it would be interesting to compare the results of this study to those of studies that are running through samples collected from other countries. Considering these limitations, our research constitutes an important stepping-stone for future research in different national settings in which it involves an investigation of the factors that influence e-payment security and trust. Second, the use of a particular e-payment method is likely to influence the sample respondents in their answers. In our research, credit and debit cards accounted for more than 90% of EPS usage in the samples. Although credit and debit cards entail similar procedures to other e-payment methods, the dominance of these two modes of payment necessitates a careful explanation of our results. Third, although the research comes up with some significant findings from the view point of consumers, it does not include all the factors that affect consumers' use of EPS. For example, factors, such as e-payment functions and individual factors can be taken into consideration in future research.

REFERENCES

Abrazhevich, D., 2004. Electronic Payment Systems: A User-Centered Perspective and Interaction Design.Technische Universiteit Eindhoven, Eindhoven, pp: 24-26.

Akerlof, G., 1970. The market for lemons: Quality uncertainty and the market mechanism. Q. J. Econ., 84(3): 488-500.

Chellappa, R. and P. Pavlou, 2002. Observed information security, financial liability and consumer trust in electronic commerce arrangements. Logistics Inf. Manage., 15(5): 358-368.

Chou, Y., C. Lee and J. Chung, 2004. Understanding M-commerce payment systems through the analytic hierarchy process. J. Bus. Res., 57: 1423-1430.

Cotteleer, M.J., C.A. Cotteleer and A. Prochnow, 2007. Cutting checks: Challenges and choices in B2B e-payments. Commun. ACM, 50(6): 56-61.

Culnan, M.J. and P.K. Armstrong, 1999. Information isolation concerns, procedural fairness and impersonal trust: An empirical investigation. Organ. Sci., 10: 104-115.

Dai, X. and J. Grundy, 2007. NetPay: An off-line, decentralized micro-payment system for thin-client applications. Electron. Commer. R. A., 6: 91-101.

Egger, F.N. and D. Abrazhevich, 2001. Security and trust: Taking care of the human factor. Electronic Payment Systems Observatory Newsletter, Vol. 9.

Friedman, B., D. Hurley, D.C. Howe, E. Felten and H. Nissenbaum, 2002. Users' Conceptions of Web Security: A Comparative Study. In Proceedings of the CHI: Changing the World, Changing Ourselves, ACM Press, Minnesota, USA, April 20-25.

Gefen, D., D.W. Straub and M.C. Boudreau, 2000. Structural equation modeling and regression: Guidelines for research practice. Commun. Associ. Inf. Syst., 6 (Article 7): 1-30.

Gerbing, D.W., J.C. Anderson and M. Carlo, 1993. Evaluation of goodness-of-fit indices for structural equations models. Sociolog. Method Res., 21(2): 132-160.

Hair, J.F., R.E. Anderson, R.L. Tatham and W.C. Black, 2003. Multivariate Data Analysis. 5th Edn., Pearson Education, India.

Hegarty, J., *et al*., 2003. A trust model for consumer internet shopping. Int. J. Electron. Comm., 6(1): 75-91.

Herzberg, A., 2003. Payments and banking with mobile personal devices. Commun. ACM, 46: 53-58.

Hsieh, C., 2001. E-commerce payment systems: Critical issues and management strategies. Hum. Syst. Manage., 20: 131-138.

Hwang, R., S. Shiau and D.A Jan, 2007. New mobile payment scheme for roaming services. Electron. Commer. R. A., 6: 184-191.

Jewson, R., 2001. E-Payments: Credit Cards on the Internet, White Paper, 1-7. Retrieved from: www.aconite.net, (Accessed on: January 04, 2009).

Joreskog, K.G. and D. Sorbom, 1993. LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language: Scientific International Software. Chicago, IL.

Kalakota, R. and A.B. Whinston, 1996. Frontiers of Electronic Commerce. Addison Wesley Publishing, Country.

Kalakota, R. and A.B. Whinston, 1997. Readings in Electronic Commerce. Addison Wesley Publishing, Reeding, Mass.

Kim, J.B., H. Kim and W. Lee, 2006. An empirical study on settlement risks of payment and settlement system in Iran. J. Financ. Investigation (Irann), 10: 1-178.

Kline, R.B., 1998. Principles and Practice of Structural Equation Modeling. The Guilford Press, New York.

Kniberg, H., 2002. What makes a micropayment solution succeed. M.A. Thesis, Institution for Applied Information Technology, Stockholm, Sweden.

Kousaridas, A., G. Parissis and T. Apostolopoulos, 2008. An open financial services architecture based on the use of intelligent mobile devices. Electron. Commer. Res. Appl., 7: 232-246.

Laudon, K.C. and C.G. Traver, 2001. E-Commerce: Business, Technology, Society. Addison Wesley Publishing, Halethorpe, MD

Lawrence, E., S. Newton, B. Corbitt, R. Braithwaite and C. Parker, 2002. Technology of Internet Business. John Wiley and Sons Australia Publishing, Brisbane.

Lim, A.S., 2008. Inter-consortia battles in mobile payments standardization. Electron. Commer. R. A., 7: 202-213.

Lin, J. and H. Lu, 2000. Towards an understanding of the behavioural intention to use a website. Int. J. Inform. Manage., 20: 197-208.

Linck, K., K. Pousttchi, D.G. Wiedemann, 2006. Security issues in mobile payment from the customer viewpoint. In Proceedings of the 14th European Conference on Information Systems (ECIS 2006), Goteborg, Schweden, pp: 1-11.

Mallat, N., 2007. Exploring consumer adoption of mobile payments-a qualitative study. J. Strategic Inf. Syst., 16: 413-432.

Miyazaki, J. and K. Fernandez, 2000. The antecedents and consequences of trust in online purchase decisions. J. Interact. Mark., 16(2): 47-63.

Mukherjee, A. and P. Nath, 2003. A model of trust in online relationship banking. Int. J. Bank Market., 21(1): 5-15.

Novak, T.P., D.L. Huffman and Y.F. Yung, 2000. Measuring the customer experience in online environments: A structural modeling approach. Market. Sci., 19(1): 22-35.

Nunnally, J.C., 1978. Psychometric Theory. McGraw-Hill, New York, pp: 23-45.

Peha, J.M. and I.M. Khamitov, 2004. Pay Cash: A secure efficient internet payment system. Electron. Commer. Res. Appl., 3: 381-388.

Pilioura, T. 2001. Electronic Payment Systems on Open Computer Networks: A study. Computer and Information Science Publications Collection,pp: 197-227.

Romdhane, C., 2005. Security implications of electronic commerce: A study of consumers and businesses. Int. Res. Electr. Networking Appl. and Policy, 9(5): 372-382.

Schneider, G., 2007. Electronic Commerce. Thomson Course Technology, Canada.

Slyke, C. V. and F. Belanger, 2003. E-Business Technologies: Supporting the Net-Enhanced Organization. John Wiley and Sons Inc., New yark.

Steiger, J.H., 1990 Structural model evaluation and modification:An interval estimation approach. Mult. Behav. Res., 25: 173-180.

Stroborn, K., A. Heitmann, K. Leibold and G. Frank, 2004. Internet payments in Germany: A classificatory framework and empirical evidence. J. Bus. Res., 57: 1431-1437.

Theodosios, T. and S. George, 2005. Concept of security and trust in electronic payments. Comput. Security, 24 (1): 10-15.

Tsiakis, T. and G. Sthephanides, 2005. The concept of security and trust in electronicpayments. Comput. Security, 24: 10-15.

Weir, C.S., J.N. Anderson and M.A. Jack, 2006. On the role of metaphor and language in design of third party payments in banking: Usability and quality. Int. J. Hum-Comput. St., 64(8): 70-784.

Wright, D., 2002. Comparative evaluation of electronic payment systems. INFOR, 35(1): 71-85.