J. Basic. Appl. Sci. Res., 2(2)1575-1581, 2012

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

An Investigation about Customers Perceptions of Security and Trust in E-Payment Systems among Iranian Online Consumers

Kambiz Heidarzadeh Hanzaee[1] and Somayeh Alinejad[2]

Department of Business Management, Science and Research Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Few studies have addressed payment issues related to online banking in Iran. This paper examined issues specifically related to e-payment security from the viewpoint of customers, proposing a conceptual model that delineates the determinants of consumers' perceived security and perceived trust as well as the effects of perceived security and perceived trust on the use of e-payment systems. The study employed structural equation modeling with data collected from 210 online respondents in Iran. The results demonstrated that technical protections and transaction procedures were positively associated with consumers' perceived security and trust in e-payment systems. In addition, experience from trusted sources of information was positively associated with consumers' perceived trust in e-payment systems. The findings further showed that perceived security in e-payment systems was positively associated with consumers' perceived trust in e-payment systems and the effects of consumers' perceived security and trust in e-payment systems were positively associated with e-payment systems use.

KEYWORDS: Electronic payment systems (EPS), EPS use, Security in EPS, Trust in EPS, Word of mouth.

INTRODUCTION

Generally defined, electronic payment (e-payment) is a form of a financial exchange that takes place between the buyer and seller facilitated by means of electronic communications. Electronic payment systems (EPSs) are utilized to facilitate the most important action after the customer's decision to pay for a product or service—namely, to deliver payments from customers to vendors in the most effective, efficient, and problem-free way. The need for online payments was first addressed by using extant payment methods of the offline world for online payments. [1]

Compared to the traditional payment methods, e-payment techniques have several favorable characteristics, including security, reliability, scalability, anonymity, acceptability, privacy, efficiency, and convenience. EPSs' increasing recognition has resulted in them being deployed throughout the world. Countries such as France, the US, and the UK have fully developed systems, while regions such as the Asia–Pacific rim provide the growth impetus to the industry.

Effective EPSs have a number of advantages over the traditional payment methods, yet they must be free of security breaches. [2] As the number of products and services offered via the Internet rapidly grows, consumers are becoming increasingly concerned about security issues. [3] Generally, security is a set of procedures, mechanisms, and computer programs for authenticating the source of information and guaranteeing the process. A number of EPSs have recently emerged on the Internet; although various security measures and mechanisms have been designed for these EPSs, many security problems remain. Hence, there is a growing need to minimize the risks associated with e-payment transaction processes. As the majority of EPS users are relatively unfamiliar with the technical details of the systems, they tend to evaluate the security level of the EPS based on of their experience with user interfaces.

Thus, to attract and retain e-payment users, it is vital to enhance consumers' perceptions of security and maintain customers' trust during e-payment transactions. [2] The e-payment process is considered confidential when all phases of the process satisfy the needs of participants and their security expectations. A fundamental prerequisite must be that all participants have absolute trust in the system in which they participate. The contraction of trust in an e-payment system must take into consideration data, identities, and role behavior. The adoption of e-commerce must consider trust and risk as important determinants of adoption behavior. [4]

However, limited published work has explored the factors that influence security and trust of Internet banking from the perspectives of customers in the context of developing countries in the Middle East. Thus, the current paper focuses upon Iran, which has a diverse population, a legal system, and a developing economy, thereby making it an interesting and unique case study.

***Corresponding Author:** Kambiz Heidarzadeh Hanzaee , Department of Business Management, Science and Research Branch, Islamic Azad University, Tehran, Iran, Email: heidarzadeh@srbiau.ac.ir Tel: +9821 44869667

LITERATURE REVIEW

Electronic Payment Systems

E-payment is defined here 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 access and manage their bank accounts and transactions remotely. [2]The principal classification of EPSs is based on the form of money representation and the principle of money transfer. Existing payment systems can be divided into two groups: electronic cash mechanisms (or electronic currency) and credit-debit systems. Electronic cash resembles conventional cash, as parties exchange electronic tokens that represent value, just as banknotes and coins determine the nominal value of conventional cash money. The credit-debit approach in the context of electronic payments means that money is represented by records in bank accounts; this information is electronically transferred between parties over computer networks. [1]Payment systems can be classified in a variety of ways according to their characteristics, such as the exchange model (cash-like, check-like, or a hybrid), central authority contact (online or offline), or hardware requirements (specific or general). We provide a brief introduction of two typical payment schemes adopted as the underlying payment mechanisms in our architecture.

1- Secure Electronic Transaction (SET)

Currently, a common e-payment method involves a client transmitting detailed information of his payment card (e.g., a Visa credit card) to a merchant. This system is simple, but susceptible to fraud from either transacting party.

The Secure Electronic Transaction (SET) protocol is an evolution of the existing credit card-based payment systems.

It provides enhanced security for information transfer as well as authentication of transaction participant identities through registration and certification. It has the potential to become a de facto international standard.

2- Digital Cash (E-Cash)

Participants of electronic currency payment systems include payers (buyers), merchants, and financial institutions.

Digital cash uses an electronic token (usually a unique coded string) to represent monetary value. The bank issuing the tokens maintains a record of all the tokens. The acquiring bank of the merchants that receive the tokens will transfer them to a clearinghouse to process them. When the tokens are verified by the issuing bank, the real transaction of funds will take place and the tokens cannot be used again. The usage of digital cash enables full anonymity that cannot be found in other payment systems. Published schemes include E-Cash and Net Cash. [5]

Review of the literature on security and trust issues in EPS

In order to identify the factors that affect consumers' perceived security and perceived trust in the use of EPS in B2C and C2C EC, this section reviews the relevant literature and provides a conceptual foundation.

Consumers' trust in their online transactions is important and has been identified as a key to the development of ecommerce.

The issue of trust is more important in online as opposed to offline banking. Many researchers agree that trust is more important in online banking because transactions of this nature contain sensitive information and parties involved in the financial transaction are concerned about access to critical files and information transferred via the Internet. [6]

Since the Internet is an open network with no direct human control over individual transactions, the technical infrastructure that supports EC and EPS must be resistant to security attacks. Technical protections devised to reduce such risk need to be considered before the problem of consumer trust is addressed. Researchers assess some of the issues associated with the security of EPS, noting that EPS should be hardened against security breaches and that the vulnerability of EPS should be carefully considered. The security of e-payment transactions depends on a number of factors, including systems factors such as technical infrastructure and implementation, transaction factors such as secure payment in accordance with specific and well defined rules, and legal factors such as a legal framework for electronic transactions. Reviewing existing security technologies for EPS, including encryption and authentication techniques, some researchers conclude that a secure e-payment system should provide security against fraudulent activities and must protect the privacy of consumers. Finally, researchers addresses the importance of security evaluation for EPS and argues that a secure EPS must incorporate two components: (1) integrity, which encompasses authentication, fraud prevention, and privacy; and (2) divisibility, transferability, duplicate spending prevention, payment confidentiality, payment anonymity, and payer traceability.

Transaction procedures in EPS have also been discussed at length in prior literature. The procedures in e-payment solutions differ from those in the traditional payment solutions because the transaction infrastructures are

fundamentally different from each other; this may engender a range of new security issues, including concerns over unauthorized use and transaction status. Although an EPS has the advantage of overcoming time and space constraints compared to the traditional offline transactions, consumers' perceptions of security and the trust they place in systems are of paramount importance for increasing the use of these systems. Some researchers argue that sophisticated procedures and process interactions should be developed in EPS to deal with security requirements. They also suggest that refined process interactions in EPS can eliminate consumers' fears over security issues associated with the use of EPS. Posting security statements on e-payment sites is another important step; here "security statements" refers to the information provided to consumers for EPS operations and security solutions. However, few studies address the importance of security statements in EPS. Researchers argue that security-related statements posted on websites are likely to increase the chances of consumers' purchasing and paying over the Internet.

The rationale supporting this proposition is based in the concept of information asymmetry and the role that it plays in decision-making. Information asymmetry refers to situations in which one of the parties involved in a transaction does not have access to all the information needed for decision making, which has been recognized as one of the major problems in EPS. The extent of information asymmetry (i.e., security statements not provided to customers) should influence customers' perceptions of security and trust in EPS.

Researchers also suggest that statements detailing security features, data protection and privacy, security policies, and other descriptive contents concerning safety precautions help users construct more accurate interpretations of what a secure EPS is.

Consumers are extremely sensitive to the risks involved in personal privacy and information security. A great deal of prior empirical research has focused on the technical details of protection, such as privacy and integrity, which are critical for consumers' use of EPS. However, transaction procedures for authentication, confirmation, and modification are also important in EPS. Furthermore, the availability, accessibility, and comprehensibility of security statements are vital for e-payment transactions. All three of these dimensions should be considered in the design of secure EPS.

Based on this literature review, we can categorize the factors that influence consumers' perceptions of security and trust in the use of EPS into three areas: security statements, transaction procedures, and technical protections. As previously described, security statements refer to the information provided to consumers in association with EPS operation and security solutions. Technical protections refer to specific and technical mechanisms to protect consumers' transaction security. Transaction procedures refer to the steps designed to facilitate consumers' actions and eliminate their security fears. [2] In addition, pre-interaction factors, including experience from trusted sources of information (e.g., word of mouth and traditional media), influence perceived trust in EPS. [7]

In this paper, we aim to examine issues related to e-payment security from customers' perspective. This study proposes a conceptual model that delineates the determinants of consumers' perceived security and perceived trust as well as the effects of perceived security and perceived trust in EPS use.

Hypotheses

Hypothesis1. Technical protections are positively associated with consumers' perceived security in EPS.
Hypothesis2. Technical protections are positively associated with consumers' perceived trust in EPS.
Hypothesis3. Transaction procedures are positively associated with consumers' perceived security in EPS.
Hypothesis4. Transaction procedures are positively associated with consumers' perceived trust in EPS.
Hypothesis5. Security statements are positively associated with consumers' perceived security in EPS.
Hypothesis6. Security statements are positively associated with consumers' perceived trust in EPS.
Hypothesis7. Experience from trusted sources of information is positively associated with consumers' perceived trust in EPS.
Hypothesis8. Perceived security in EPS is positively associated with consumers' perceived trust in EPS.
Hypothesis9. Perceived security in EPS is positively associated with consumers' use of EPS.
Hypothesis10. Perceived trust in EPS is positively associated with consumers' use of EPS.

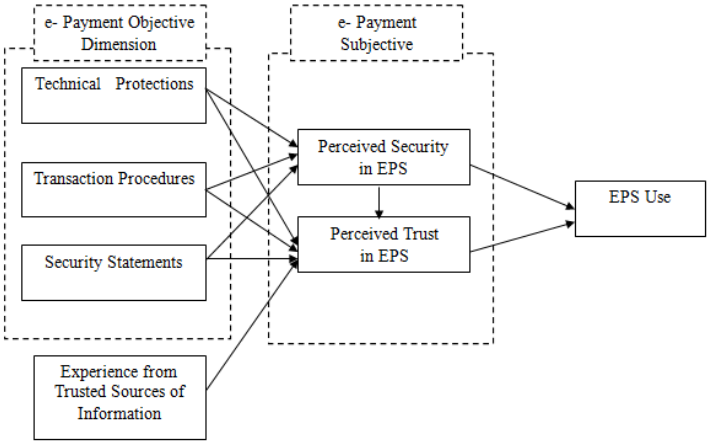


Figure1. The proposed model

Materials and Methods

To test the theoretical framework, we examined online consumers' perceptions about trust and security related to internet payment.

Sampling

Research participants are people familiar with the internet who use internet banking. Online consumers are generally younger and more educated than conventional consumers. A questionnaire was sent to participants; 250 responses were received. After eliminating incomplete and inappropriate responses (e.g., duplicates), 210 usable responses were included in the sample for construct validation and hypothesis testing. The data collected indicated that the participants were active online consumers.

Measurements

Measurement items used in this study were adapted from previously validated measures or were developed based on the literature review. [2],[7] This research measures technical protections using three categories: privacy, integrity, and confidentiality. A privacy-protection mechanism can reassure consumers that their personal information, such as names, addresses, and contact details, will not be released to other parties. Meanwhile, this research measures transaction procedures using three factors: authentication, modification, and confirmation. Authentication is the procedure by which the identity of participants is verified through their identity and password before they participate in an EPS. Modification is the procedure by which consumers cancel or modify their payment amount or method prior to the completion of the final stage of the payment process. Confirmation is the procedure by which consumers can be assured that their payments have been received by merchants. Finally, this research measures security statements using three factors (i.e., availability, accessibility, and comprehensibility) as well as experience from trusted sources of information using two factors (i.e., word of mouth and information from neutral sources).

Responses were evaluated on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

RESULTS AND DISCUSSION

Measurement Model

Researchers have reached consensus that validity is the most important concept in measurement; thus, the measurement scale in the current study was first tested for reliability and validity while the path model was subsequently assessed using SEM for hypothesis testing. To test the validity of the measurement used, confirmatory factor analysis (CFA) was employed to assess, develop, and modify the proposed theoretical model. Here, a series of CFA that utilized maximum likelihood estimations to test measurement model were carried out for each of seven latent variables (i.e., technical protections, transaction procedures, security statements, experience from trusted sources of information, perceived security in EPS, perceived trust in EPS, and EPS use). To ensure an acceptable model fit, the measurement was tested for unidimensionality, reliability, and validity. To improve the model, a series of modifications were made based on items' reliability, modification index, and standard residuals. The candidate items were removed from the model, and a proper model fit was reached (see Table 1). As Table 1 indicates, the $\chi 2/df$ is less than the threshold of 3, which guarantees an adequate model fit. The CFI and GFI values produced by

the model are 0.957 and 0.911, respectively, satisfying the fit requirement. RMSEA and SRMR were both less than 0.08, ensuring the proper unidimensionality for the measurement model. The validity and reliability of the model can be assessed based on the composite reliability and AVE, which are described in Table 2.

Table 1: Fit Statistics & Indexes for measurement model of EPS Use

	χ2	Df	P<0.001	χ2/df	GFI	CFI	RMSEA	SRMR
Second-order	733.260	303	0.000	2.420	0.911	0.957	0.059	0.050

Table 2: Number of items, Cronbach's alpha, items deleted, Composite Reliability and Average Variance Extracted (Measurement Model)

Constructs	Number of items	Cronbach's alpha	Composite Reliability	AVE
Technical Protections	6	0.88	0.81	0.74
Transaction Procedures	4	0.77	0.74	0.69
Security Statements	3	0.88	0.81	0.77
Experience from Trusted Sources of Information	5	0.80	0.81	0.75
Perceived Security in EPS	3	0.85	0.80	0.71
Perceived Trust in EPS	3	0.81	0.84	0.79
EPS Use	3	0.75	0.81	0.74

As Table 2 indicates, AVE for all constructs was above 0.5, demonstrating the model's construct reliability. The Cronbach's alpha and composite reliability were both above the acceptable cut-point of 0.6, ensuring the reliability of constructs in the measurement model. On the other hand, discriminant validity is established if the AVE score is higher than the squared correlation shared between two variables (see Table 2). The results for the constructs' discriminant validity are shown in Table 3.

Table 3: Results of Average Variance Extracted and Squared Correlations of Each Construct

Constructs	1	2	3	4	5	6	7
Technical Protections	0.74						
Transaction Procedures	0.23	0.69					
Security Statements	0.13	0.20	0.77				
Experience from Trusted Sources of Information	0.29	0.29	0.17	0.75			
Perceived Security in EPS	0.18	0.12	0.03	0.14	0.71		
Perceived Trust in EPS	0.23	0.19	0.07	0.18	0.32	0.79	
EPS Use	0.32	0.28	0.21	0.26	0.37	0.39	0.74

The AVE values are reported diagonally while the squared correlations values are shown below the diagonal. The results demonstrate that the lowest average AVE value is 0.69 (transaction procedures); none of the squared correlation values fall above this score. This indicates that all seven variables utilized in this study were distinct constructs, indicating the existence of discriminant validity (see Table 3).

Structural Model

The proposed structural model for this study is shown in Figure 1. As illustrated, four independent variables (technical protections, transaction procedures, security statements, experience from trusted sources of information) and two mediating ones (perceived security in EPS, perceived trust in EPS) are included. The dependent variable is EPS use (see Figure 1).

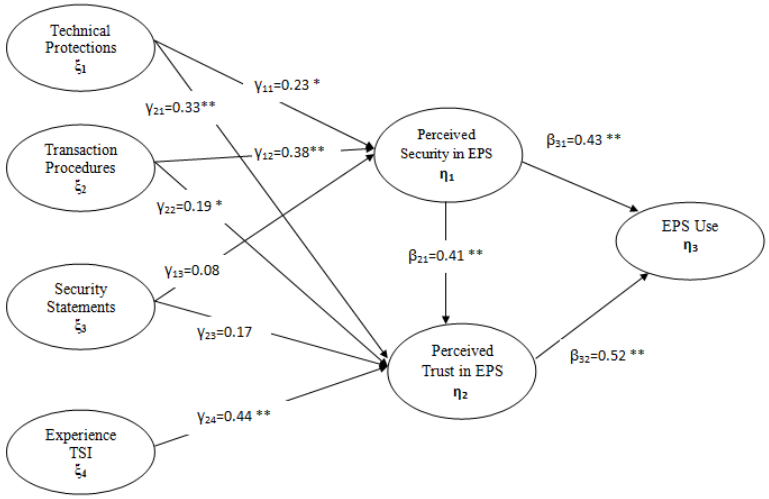
The data set may have many feasible fit models, just as more than one theory may explain a phenomenon that occurs in society. However, it is not always certain which explanation is best. Thus, we used model competition to determine the best among comparative models. Two competitive models—the completely mediating model (model B) and the direct effect model (model C)—were compared with the partially mediating model (model A). The results are shown in Table 4.

For the completely mediating model (model B) and partially mediating model (model A), all the fitted indices of GFI, NFI, SRMR, and RMSEA were consistent while the __2 was insignificant. According to the parsimonious principle, it can be concluded that the completely mediating model (model B) is the best choice (see Table 4). The estimated path coefficients of the completely mediating model are shown in Figure 2.

Table4. Model competition results

Model	$\chi 2$	Df	$\Delta\chi^2$	GFI	NFI	RMSEA	SRMR
Model A[a]		233	-	0.901	0.942	0.056	0.051
Model B[b]		237	3.67	0.903	0.943	0.055	0.050
Model C[c]		237	110.29	0.89	0.920	0.081	0.079

a: Partially mediating model. b:Completely mediating model. c: Direct model.



*p<0.01
**p<0.05

Figure 2.Result of completely mediating model

Results of Hypothesis Testing

The results of the structural coefficients exhibited in Figure 2 were used to examine the hypotheses of this study. Hypothesis 1 states that technical protections are positively associated with consumers' perceived security in EPS.

As Figure 2 illustrates, the path from technical protections to consumers' perceived security in EPS yielded a significant coefficient value of 0.23 ($p>0.05$), which means that this hypothesis is supported by the findings. In addition, the path between technical protections and perceived trust in EPS had a value of 0.33, significant at the 0.01 level, thereby confirming hypothesis 2. As shown in Figure 2, the link between transaction procedures and consumers' perceived security in EPS generated a coefficient value of 0.38 and was significant at the 0.01 level.

Thus, it can be inferred that transaction procedures have a significant positive effect on consumers' perceived security in EPS, supporting the third hypothesis. Hypothesis 4 states that a positive relationship exists between transaction procedures and consumers' perceived trust in EPS. With a coefficient path of 0.19 ($p<0.05$) between these two variables, this hypothesis is also supported by the findings. However, as shown in Table 5, hypothesis 5 is not supported by the data as the coefficient value for the route from security statements to consumers' perceived security in EPS was not significant at the 0.05 level.

The same is true of the effect of security statements on consumers' perceived trust in EPS. Thus, security statements have no significant positive effect on consumers' perceived security in EPS (hypothesis 5) nor consumers' perceived trust in EPS (hypothesis 6). Hypothesis 7 is concerned with the effect of experience from trusted sources of information on consumers' perceived trust in EPS. As demonstrated in Table 5, the relationship between the two was 0.44 and was significant at the 0.01 level. Hence, it can be inferred that hypothesis 7 is also supported by the findings of this study. The findings further indicated that perceived security in EPS is positively associated with consumers' perceived trust in EPS; the path value for this route was 0.41, indicating that hypothesis 8 is also confirmed. The last two hypotheses of this study concern the effects of consumers' perceived security in EPS and consumers' perceived trust in EPS on EPS use. As Table 5 highlights, both paths were significant at the 0.01 level, with coefficient values of 0.43 and 0.52 respectively (see Table 5).

Table5. Path coefficients for the structural model

Path		coefficient	t-value	significance
From	to			
technical protections	consumers'perceived security in EPS	0.23	2.98	P<0.01
technical protections	consumers' perceived trust in EPS	0.33	3.44	P<0.01
transaction procedures	consumers' perceived security in EPS	0.38	3.80	P<0.01
transaction procedures	consumers' perceived trust in EPS	0.19	1.93	P<0.05
security statements	consumers' perceived security in EPS	0.08	1.01	p>0.05
security statements	consumers' perceived trust in EPS	0.17	1.29	p>0.05
experience from trusted sources of information	consumers' perceived trust in EPS	0.44	4.28	P<0.01
consumers' perceived security in EPS	consumers' perceived trust in EPS	0.41	3.91	P<0.01
consumers' perceived security in EPS	EPS use	0.43	4.17	P<0.01
consumers' perceived trust in EPS	EPS use	0.52	4.80	P<0.01

Conclusions

This paper examines security issues in the context of EPS from consumers' perspectives. Our research proposed a research model that delineates the determinants of consumers' perceived security and perceived trust as well as the effects of perceived security and perceived trust on EPS use. Our findings indicate that both technical protections and transaction procedures are significant factors for improving consumers' perceived security. Consumers' perceived security is positively related to consumers' perceived trust and EPS use. Finally, consumers' perceived trust also has a positive impact on EPS use. Some of the results from this study are not consistent with the results of previous research by researchers. [2] Indeed, the current study found no evidence of a statistically significant relationship between the security statements and consumers' perceived security or perceived trust in EPS use.

Yet this study provides important theoretical and practical contributions to the area of security and trust in EPS. It developed a theoretical model of consumers' perceived security and perceived trust, including their roles in the use of EPS. It further helped explain the direct relationships between perceived security, perceived trust, and EPS use.

Our results clearly delineate the role of consumers' perceived security in building trust among consumers and the positive impact of both perceived security and perceived trust on EPS use. The effects of experience from trusted sources of information on consumers' perceptions of trust were also validated. Consumers' perceived security and perceived trust are essential concepts in our understanding of consumers' use of EPS. This research is consistent with previous claims that both perceived security and perceived trust perform a crucial function in promoting consumers' EPS use.

REFERENCES

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

[2] Kim, Changsu, Wang Tao, Namchul Shin and Ki-Soo Kim, 2010. An Empirical Study of Customers' Perceptions of Security and Trust in E-payment Systems. Electronic Commerce Research and Applications, 9: 84-95.

[3] Agarwal, Reeti, Sanjay Rastogi and Ankit Mehrotra, 2009. Customers' Perspectives Regarding E-banking in an Emerging Economy. Journal of Retailing and Consumer Services, 16: 340-351.

[4] Tsiakis, T. and G. Sthephanides, 2005. The Concept of Security and Trust in Electronic Payments. Computers and Security, 24: 10-15.

[5] Guan, Sheng-Uei and Feng Hua, 2000. A Multi-Agent Architecture for Electronic Payment. Consumer Affairs, 15: 1-38.

[6] Al-Somali, Sabah Abdullah, Roya Gholami and Ben Clegg, 2009. An Investigation into the Acceptance of Online Banking in Saudi Arabia. Technovation, 29: 130-141.

[7] Walczuch,Rita and Henriette Lundgren, 2004. Psychological Antecedents of Institution-Based Consumer Trust in E-retailing. Information & Management, 42: 159-177.