DETERMINANTS OF E-PAYMENT SYSTEM PERCEPTION AND SATISFACTION: JOURNEY FROM INDIA TO CANADA

Arushi Jain*

*Research Scholar,
University of Delhi,
Delhi City, INDIA
Email id: jainarushi74@gmail.com

ABSTRACT

Canada is the country, most embracing cashless technology hardly surprising since there are over 2 credit cards for every person living there as claimed by a recent study of forex bonuses 2017. In 2016 this position was attained by Sweden, where barely 1% of the value of all payments was paid in coins or notes. Is India still on the verge of being known as "yet to become a cashless economy"? If yes, then how much time does India expect to become a cashless economy. It is commonly believed that good security gains public trust, and the perceptions of good security and trust ultimately increase the use of electronic payment system. In this paper, we examine the relationship between the security measures offered by the e-payment channel and the ultimate perception of the consumers of the security, trust and usefulness of the e-payment system this study proposes an empirical model that delineates the factors of consumers' perceived security and perceived trust, with the effects of perceived security and perceived trust on the use of e-payment systems. Primary data has been collected through questionnaires and hypothesis testing is done. Our results show that transaction procedure significantly impacts the perception of the customers which can be employed by the service providers to make e payment sources more efficient and increase its usage.

KEYWORDS: *E Payment, Perception, Security, Trust.*

1. INTRODUCTION

This paper examines individual users' experience of electronic payment systems (e-payment system). Due to its widely accepted benefits, many businesses are accepting e-payment systems for commercial transactions. E-payment system has been researched with increasing interest and depth. India specifically provides an interesting case with its demonetization to motivate individuals to experience e-payment system as it is currently integrating the governmental organizations to an online system and, at the same time an increasing number of businesses are using e-payment system for their daily transactions. The individual user's experiences of customers in India are essential as per the provided data from questionnaires besides enriching the current usage, gives a clear perspective for practitioners such as businesses, advertising, hr and marketing agencies and financial institutions using e-payment system services. A number of e-payment systems have recently emerged for the public usage. But various security measures and transaction mechanisms have been designed which often comes with many security problems. Hence, there is a need to reduce and minimize the risks associated with e-payment processes. The majority of users of e-payment system are young generation who is well versed with the process of using e-payment system but the older generation and illiterate are relatively unfamiliar with the

technicalities of e-payment system, and hence they tend to evaluate the security level of e-payment system on the basis of their experience with their close ones and feel safe and confident while using e-payment system (Kaur 2015 **[1]**) thus, to increase and retain e-payment users, it is important to enhance consumers' perceptions of security and maintain customers' trust during e-payment transactions. The principal objective of this study is to empirically examine, from the viewpoint of users, the main factors that affect their perceptions of security and trust of e-payment system. In the next section, the e-payment system has been used and in the subsequent section data analysis has been done win context of prior research on security and trust issues in e-payment system following this section, a literature review with a historical framework is presented with the underlined hypotheses after which, the research methodology and findings are discussed. Finally, conclusions are provided in the last section.

2. LITERATURE REVIEW

The expanding use and commercialization of the internet have prompted a dynamic web-based business world. Lee, yu, and ku (2001) **[2]** states that electronic business gives various points of interest over conventional trade for e.g. Straightforwardness, speed, obscurity and worldwide openness, which improve and upgrade people's personal satisfaction. These advantages help the ubiquity of e-trade and gives the aggressive edge to the organizations which embrace it. Despite the fact that e-installment framework has improved and upgraded essentially in the course of the most recent decade, some security and trust issues are as yet a matter of worry for clients (Shon and Swatman, 1998 **[3]**). As per a few scientists, for example, van dyke, Midha, and Nemati (2007) **[4]** and Wu and wang (2005) **[5],** trust and security are the two principle columns that avert people taking part in internet business exchanges need to utilize it.

Exchange technique has been recognized as a factor significantly impacting the security and trust factor in e-installment framework (Hwang, li, and Hsiao, 2006 **[6]**; Kim et al., 2010 **[7]**). Specialized securities given by the stage suppliers have been named as the significant predecessors for e-installment framework. Chellappa (2002) **[8]** says that specialized insurances positively affect apparent security and trust. At the end of the day, giving adequate and persuading specialized insurance estimates will upgrade buyers view of security and trust in e-installment. As per Hwang, Shiau, and Jan et al. (2010) **[9],** exchange systems whenever depicted legitimately help people to decrease their security concerns.

Security proclamations in e-installment framework have been observed to be a significant factor impacting customer's trust in e-installment framework. (Mukherjee and Nath, 2003) **[10].** Miyazaki and Fernandez (2000) **[11]** expressed that security articulations given on e-installment framework will improve the probability of customers utilization of the internet. Past experience will prompt the quicker reception and utilization of new advancements (i.e e-installment framework.) (Wu and wang, 2005) **[5].** Kim et al. (2010) **[7]** have characterized seen security as the customer's reason for assessment of the e-installment framework's security. Also, Tsiakis and Sthephanides (2005) **[12]** have characterized seen trust as shoppers' conviction that electronic installment exchanges will be continue as per their desires. Client's involvement with e-installment framework. Was estimated with a five-thing scale, which was created by the concerned creators with the end goal of their investigation. The seven-point likert-type reaction classes were- 1=strongly dissent; 7=strongly concur were utilized. The examination estimated the specialized insurances by means of protection; trustworthiness of the-installment framework through certain components and by privacy; exchange methods by means of validation as given by the e-installment stage suppliers together with affirmation and security articulations estimated by accessibility; availability; and understandability measures (Kim et al., 2010) **[7].**

A few discoveries have appeared seen security and seen trust together have a positive and critical effect on e-installment framework likelihood of utilization i.e., when the clients see the e-

Asian Journal of Research in Social Sciences and Humanities
ISSN: 2249-7315   Vol. 12, Issue 03, March 2022   SJIF 2022 = 8.625
A peer reviewed journal

installment framework as secure, dependable and simple to utilize, they are additionally eager to process their exchanges electronically. These outcomes are steady with the writing (Culnan and Armstrong, 1999 [13]). A few outcomes have likewise appeared specialized insurance gives the most grounded base of both saw security and trust. This finding is steady with one examination e.g, Kim et al., 2010. Exchange methodology in e-installment framework has likewise been talked about in incredible profundity in some earlier writing (for example Linck et al. 2006 [14], Dahlberg, et al. 2008 [15]). Miyazaki and Fernandez (2000) [11] states that security articulations posted on sites are probably going to improve the odds of customer's buying and paying over the internet stages. The thought supporting the expressed suggestion has its premise in the data asymmetry and the job that is played in basic leadership by the clients. Data asymmetry is a case in which one of the gatherings associated with an exchange doesn't approach all the data required for basic leadership (Anderson and Gerbing, 1988 [16]). This has been perceived as one of the serious issues blocking the advancement of e-installment framework.
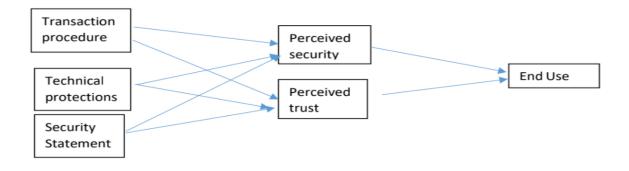
3. RESEARCH METHODOLOGY

3.1 Sample

This study considers the frequency and the satisfaction level with which customers use e-payment system and their satisfactory level. Therefore, an online questionnaire has been used to collect data. In total 263 questionnaires were responded, out of those collected responses, a significant response rate of 98.6%, 259 were completed fully and were appropriate to continue with the analysis.

3.2 Measures

The present study used an online questionnaire that consists of two parts, first part mainly considered personal profile of the respondents including gender and age. Last part contained some technical questions regarding respondent's experiences in using e- payment system which is divided into 6 sub sections. The questionnaire used in this study contained 20 questions regarding the respondent's usage, which are transaction procedure, technical protection, security statement, perceived security, perceived trust and extent of e-payment system use. All 20 questions included in online questionnaire were measured on a five-point Likert scale ranging from "strongly disagree = 1" to "strongly agree = 5". Research participants comprises population familiar with the internet

and who use internet banking. Online consumers are generally younger and more educated than other consumers. 85.2% of responses comprises of the population whose age lies between 18-30 years and 10.8% are those with the age lying between 31 to 45 years. 62.8% are male respondents, rest are female.

3.3 Hypothesis development

Constructs	Mean	SD
Transaction Procedure	4.069905	0.779322
Technical Protections	3.718483	0.911274
Security Statements	3.470774	0.917211
Perceived Security	3.411	0.930736
Perceived Trust	3.620853	0.854048
End Use	3.43128	1.280797

H1: there exists a significant positive relation between transaction procedure and perceived security in e-payment system

H2: there exists a significant positive relation between transaction procedure and perceived trust in e-payment system

H3: there exists a significant positive relation between the technical protection and perceived security in e-payment system

H4: there exists a significant positive relation between the technical protection and perceived trust in e-payment system

H5: there exists a significant positive relation between the security statement and perceived security in e-payment system

H6: there exists a significant positive relation between the security statement and perceived trust in e-payment system

H7: there exists a significant positive relation between perceived security and extent of e-payment system use.

H8: there exists a significant positive relation between perceived trust and extent of e-payment system use.

3.4 Measurement Model

In this study first confirmatory factor analysis (CFA) for all 20 questions to define support for dimensionality, discriminant validity concern and convergent is performed. Aim of the test is to eliminate measures with either insignificant loading or cross-loadings. As per the previous research factor loading equal or greater than 0.5 has been chosen (Bagozzi and Yi, 1988 [17]). 1 question has been omitted as it has been having a factor loading lower than 0.5. Stata (statistical package for the social sciences) software has been used in the assessment of validity. We assessed the construct validity by identifying the concepts of the 6 constructs. In addition to this, factor scores were calculated from the identified components from the formal survey questionnaire. An exploratory factor analysis is initially conducted with rotations to detect the significance of the hypothesized factors (convergence validity).

TABLE - 2: ROTATED COMPONENT MATRIX

	Component					
	1	2	3	4	5	6
Trp1	.085					
Trp2	.168					
Trp3	-.018					
Trp4	.072					
Techp5		.023				
Techp6		.339				
Techp7		.418				
Techp8		.754				
Techp9		-.064				
Secs1			.729			
Secs2			.706			
Secs3			.611			
Ps1				.396		
Ps2				.289		
Ps3				-.004		
Pt1					.113	
Pt2					.134	
Pt3					.176	
Eu1						-.190
Eu2						.228

TABLE - 3: KMO AND BART LETT'S TEST

Kaiser-meyer-olkin measure of sampling adequacy.		.844
Bartlett's test of sphericity	Approx. Chi-square	1365.142
	Df	190
	Sig.	.000

The kmo (kaiser–meyer–olkin) values for each of the 20 survey questions exceeded 0.45. The value of the test statistic for sphericity on the basis of a chi-squared transformation of the determinant of the correlation matrix is found to be large (0.844), and the associated significance level is extremely small (0.000). We concluded that the data were approximately multivariate normal data. To determine that the 6 constructs are separate variables, a confirmatory factor analysis has been conducted through STATA with 6 components. These factors accounted for 60.01% of the variance. Table 2 shows the results of factor analysis.

Asian Journal of Research in Social Sciences and Humanities
ISSN: 2249-7315   Vol. 12, Issue 03, March 2022   SJIF 2022 = 8.625
A peer reviewed journal

TABLE 4: NUMBER OF ITEMS, CRONBACH'S ALPHA, ITEMS DELETED, COMPOSITE RELIABILITY AND AVERAGE VARIANCE EXTRACTED

Constructs	N	Chronbach alpha	Composite reliability	Ave
Transaction procedure	4	0.507	0.07207272	0.010260528
Technical protections	5	0.617	0.262077965	0.17250237
Security statements	3	0.686	0.561879777	0.468033318
Perceived security	3	0.763	0.197966921	0.08013474
Perceived trust	3	0.712	0.125975296	0.020604935
End use	2	0.503	0.019615485	0.088303624

3.5 Structural Equation Modelling

This study contains various constructs with pre-conceived directional influence on other constructs. The structural model has been used to represent the proposed hypotheses. Following test have been performed to test the fit of the model. CFI is an index of overall fit. The GFI measures the fit of a model compared to other models. The NFI measures the proportion by which a model is improved in terms of the fit when compared to the base model. The RMSEA gives the discrepancy for the degrees of freedom for a model. As per the literature, the accepted thresholds for GFI, RFI, NFI, and CFI are 0.90 and for RMSEA to be at most 0.05. These tests were performed by using structural equation modeling techniques with STATA.

TABLE 5: INDICES OF FIT AND COMMENTS FOR MODEL ANALYSIS

Indices in SEM analysis	Default model	Data fitting of the model
RMR (root mean square residual)	0.078	Good fit (should be less than 0.08)
GFI (goodness of fit index)	0.82	Not a good fit (should be greater than 0.90)
AGFI (adjusted gfi)	0.81	Good fit (should be greater than 0.80)
NFI (normed fit index)	0.82	Not a good fit (should be greater than 0.90)
RFI (relative fit index)	0.79	Not a good fit (should be greater than 0.90)
IFI (incremental fit index)	0.90	Good fit (should be greater than 0.90)
CFI (comparative fit index)	0.903	Good fit (should be greater than 0.90)
RMSEA (root mean square error of approximation)	0.055	Good fit (should be less than 0.08)

3.6 Hypotheses-Path Testing

This section provides the statistical results of the hypothesis testing. The effects of all the constructs on each other have been assessed through stata 6.0. As shown in the table 6, the effects of technical protections and security statements on consumers' perceived security in e-payment system were significant (btech = 0.019766, t = 0.361044, p<0.05 and bstat = 0.012014, t = 0.162069, p>0.05). Hence, hypothesis 3 and hypothesis 5 are supported by the results. As against this, the effect of transaction procedures on perceived security of consumers was significant (btrp

= 0.127837, t = 1.658436, p<0.05), showing that transaction procedures impact consumers' perceived security in e-payment system hence, hypothesis 1 is also supported. Moreover, these results indicate that technical protections (btech = 0.017183, t = 0.354411, p > 0.05) is not associated with consumers' perceived trust in e-payment system on the other hand, the effects of security statements (bstat = 0.078294, t = 1.196403, p<0.005) and transaction procedures on consumers' perceived trust (bproc = 0.200564, t = 2.978459, p<0.005) are significant; thus, hypothesis 6 and hypothesis 2 are supported. Our results also show that consumers' perceived security in e-payment system exerts a substantial effect on consumers' e-payment system use (btrus = -0.016444, t = -0.266131, p > 0.05), thus not supporting hypothesis 7. Finally, the impact of consumers' perceived trust in e-payment system is positively associated (bsec = 0.083004, t = 1.524684, p<0.05) with consumers' e-payment system use, thus supporting hypothesis 8.

TABLE 6: HYPOTHESES-TESTING OF THE RESEARCH MODEL

Hypothesized Path	Coefficient	Standard Error	T value	P-value
Transaction procedures - perceived security in e-payment system	0.127	0.077	1.658	0.028
Transaction procedures-perceived trust in e-payment system	0.201	0.067	2.978	0.003
Technical protections-perceived security in e-payment system	0.019	0.054	0.361	0.000
Technical protections-perceived trust in e-payment system	0.017	0.048	0.354	0.523
Security statements-perceived security in e-payment system	0.012	0.0741	0.162	0.871
Security statements-perceived trust in e-payment system	0.078	0.065	1.196	0.022
Perceived security in e-payment system-perceived trust in e-payment system	0.553	0.046	11.83	0.000
Perceived security in e-payment system-e-payment system use	-0.016	0.074	-0.266	0.790
Perceived trust in e-payment system-e-payment system use	0.083	0.083	1.524	0.008
Transaction procedures-perceived security in e-payment system	0.127	0.077	1.658	0.028
Transaction procedures-perceived trust in e-payment system	0.201	0.067	2.978	0.003
Technical protections-perceived security in e-payment system	0.019	0.054	0.361	0.000
Technical protections-perceived trust in e-payment system	0.017	0.048	0.354	0.523
Security statements-perceived security in e-payment system	0.012	0.0741	0.162	0.871
Security statements-perceived trust in e-payment system	0.078	0.065	1.196	0.022
Perceived security in e-payment system-perceived trust in e-payment system	0.553	0.046	11.83	0.000
Perceived security in e-payment system-e-payment system use	-0.016	0.074	-0.266	0.790
Perceived trust in e-payment system-e-payment system use	0.083	0.083	1.524	0.008

The significance of the estimates is indicated by a solid line. Consumers' perceived security in e-payment system use is determined by technical protections and security statements. It is also apparent that perceived security and perceived trust are significant factors that influence consumers' e-payment system use. Additionally, there is a significant impact of perceived security on perceived trust.

4. CONCLUSION

This study examines security and trust issues in the e-payment system from the viewpoint of consumers. Our results show that both technical protections and transaction procedure are significant factors for improving consumers' perceived security. Consumers' perceived trust also has a positive impact on e-payment system use. Although negatively related to perceived security. This study finds no evidence of a statistically significant relationship between technical protections and perceived trust in e-payment system the magnitudes of the estimates are quite small, and thus do not support hypothesis 4 and hypothesis 5. One possible explanation is that complex procedures, such as cumbersome authentication and procedures, leads to fall consumers' convenience in e-payment systems. Consumers' perceptions of the e-payment system's security

and trustworthiness may be lowered as a result of the discomfort they face during technical operations. As a result, e-payment service providers may be required to provide consumers with not only safe but also convenient e-payment methods. (Tsiakis and Sthephanides, 2005 [18])

There are certain limitations to this research. To begin with, using a convenient sample confines the research's conclusions to that sample, implying that the findings cannot be applied to a broader population (Eastlick et al., 2006 [19]). If the study's goal had been to test theory, this constraint would have been an issue. However, because the primary goal of this study was to develop theory, the lack of external validity becomes less of an issue.

Consumers' perceptions of the e-payment system's security and trustworthiness may be lowered as a result of the discomfort they face during technical operations. As a result, e-payment service providers may be required to provide consumers with not only safe but also convenient e-payment methods. (Pavlou and Gefen, 2004 [20])

There are certain limitations to this research. To begin with, using a convenient sample confines the research's conclusions to that sample, implying that the findings cannot be applied to a broader population. If the study's goal had been to test theory, this constraint would have been an issue. However, because the primary goal of this study was to develop theory, the lack of external validity becomes less of an issue. Consumers' perceptions of the e-payment system's security and trustworthiness may be lowered as a result of the discomfort they face during technical operations. As a result, e-payment service providers may be required to provide consumers with not only safe but also convenient e-payment methods. (Reichheld and Schefter, 2000 [21])

Finally, the impacts of perceived security and perceived trust on e-payment system adoption were investigated separately in this study. Future research might look at the combined influence of all of these variables on the e-payment system using polynomial regression analysis. These approaches will show how the adoption of e-payment systems is connected to combinations of these predictor factors.

REFERENCES

1. Kaur K. E-payment system on e-commerce in India. Int. Journal of engineering research and application, 2015;5(2 Part I):79-87.

2. Lee ZY, Yu HC, Ku PJ. An analysis and comparison of different types of electronic payment systems. Management of engineering and technology, 2001. Picmet'01. Portland international conference on, IEEE, Portland. 20021. pp.38–45.

3. Shon TH, Swatman PM. Identifying effectiveness criteria for internet payment systems. Internet research, 1998; 8:202–218.

4. Van dyke TP, Midha V, Nmati H. The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. Electronic markets, 2007; 17:68–81.

5. Wu JH, Wang SC. (2005). What drive mobile commerce? An empirical evaluation of the revised technology acceptance model. Information and management, 2005; 42:719–729.

6. Hwang RJ, Li JF, Hsiao YK. A wireless-based authentication and anonymous channels for gsm system. Journal of computers, 2006; 17:31–36.

7. Kim C, Tao W, Shin N, Kim KS. An empirical study of customers' perceptions of security and trust in e- payment systems. Electronic commerce research and applications, 2010; 9:84–95.

8. Chellappa RK, Pavlou PA. Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics information management, 2002; 15:358–368.

9. Hwang RJ, Shiau SH, Jan DF. A new mobile payment scheme for roaming services. Electronic commerce research and applications, 2007; 6:184–191.

10. Mukherjee A, Nath P. A model of trust in online relationship banking. International journal of bank marketing, 2003; 21:5–15.

11. Miyazaki AD, Fernandez A. Internet privacy and security: an examination of online retailer disclosures. Journal of public policy; marketing, 2000; 19:54–61.

12. Tsiakis T, Sthephanides G. The concept of security and trust in electronic payments. Computers & security, 2005; 24:10–15.

13. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization science, 1999;10:104–115

14. Linck K, Pousttchi K, Wiedemann, DG. Security issues in mobile payment from the customer viewpoint. Proceedings of the 14th European conference on information systems, (ECIS 2006), Göteborg, Schweden, 2006. pp1–11.

15. Dahlberg K, Dahlberg H, Nyström M. Reflective lifeworld research (2nd ed.). Sweden: Studentlitteratur. 2008.

16. Anderson JC, Gerbing DW. Structural equation modelling in practice: a review and recommended two ste-payment system psychological bulletin, 1988;103:411–423.

17. Bagozzi RP, Yi Y. On the evaluation of structural equation models. Journal of academy of marketing science, 1988;16:74–94.

18. Tsiakis T, Sthephanides G. The concept of security and trust in electronic payments. Computers & security, 2005;24:10–15.

19. Eastlick MA, Lotz SL, Warrington P. Understanding online b-to-c relationships: an integrated model of privacy concerns, trust, and commitment. Journal of business research, 2006;59:877–886.

20. Pavlou PA, Gefen D. Building effective online marketplaces with institution-based trust. Information systems research, 2004;15:37–59.

21. Reichheld FF, Schefter P. E-loyalty. Harvard business review, 2000;78:105–113.