

Role Of Customer Perceptions In The Usage Of Electronic Payment Systems

Thirupathi Chellapalli, Daruri Venkata Srinivas Kumar

Abstract: Banking industry across the world witnessed radical transformation due to significant changes that took place in the Information Technology (IT) sector. Technological innovations made the whole world a global village and brought remarkable changes in the banking industry. Branch banking in the conventional brick and mortar mode has been transformed into click and order channel mode. The deployment of self-service technologies makes the service delivery process simple and provides the option of “do it yourself”. The dependence on electronic payment systems is growing steadily, and development of electronic commerce has given birth to electronic payment options. Electronic/ online payments played a key role the proliferation of banking and financial services. In comparison to the traditional payment methods, online payment techniques have several differentiating characteristics that include online security, reliability, acceptability, perceived usefulness, perceived ease of use, trust, convenience, etc. This paper addresses the customer perceptions related to security in online financial transactions with a specific focus on electronic banking.

Index Terms: banking services, customer perceptions, electronic banking, electronic commerce, electronic payment systems, financial services, information technology, online security

1 INTRODUCTION

Information Technology (IT) has become a necessary tool in both manufacturing and service organizations across the world. IT has ushered in new business paradigm and plays a substantial role in enhancing banking services. Indian banking industry has witnessed radical transformation due to significant changes that took place in the information technology sector. Technological changes made the whole world a global village and brought radical changes in the banking industry. Branch banking which has been in the brick and mortar mode got transformed into click and order channel mode. With the growth of e-commerce, the importance of transferring money electronically has become an important issue to marketers and consumers. The twenty-first century has witnessed dependency on information technology and as electronic transactions became part and parcel of different cross sections of society across the globe. The deployment of self-service technologies make the service delivery process simple and provide the option of “do it yourself”. The dependence on electronic payment systems is steadily growing with proliferation of business and financial services. An electronic payment system allows customers to utilize transaction facility round the year, throughout the day, that is, for 24 hours from anywhere in the world. Innovations in information technology enabled retail banking services like card banking, ATM banking, Internet banking, Mobile banking, etc. In comparison to the traditional payment methods, online payment techniques have several differentiating characteristics, security, reliability, acceptability, perceived usefulness, and perceived ease of use, trust, convenience, etc. These factors play a crucial role in the adoption and usage of electronic payment systems.

Thirupathi Chellapalli and Srinivas Kumar (2016) observed that while business organizations need to invest in infrastructure for electronic payments, it needs certain amount of learning on the side of customers to adopt to cashless transactions.

2. STATEMENT OF THE PROBLEM

Electronic payment systems are playing a vital role in delivering banking services to the customers, by enabling easy and efficient banking transactions. However, from the customers' perspective issues like transaction procedures, perceived security, and usage of electronic payment systems, etc., are challenges in the adoption of electronic payment systems. It is vital that the technology supporting electronic commerce and electronic payment systems be impervious to security attacks. In this regard, this study is done to understand customers' perceptions towards transactional procedures, technical protection, and security in electronic payment systems (Credit card banking, Debit/ATM Card Banking, Internet Banking, and Mobile Banking). This study aims to provide a conceptual foundation for understanding the role and importance of customer perceived security in online banking and the issues related to it.

3. LITERATURE REVIEW:

To identify the factors that affect consumer's perceived security in the use of electronic payment systems in B2B and C2C transactions, etc., literature about various studies related to electronic payment systems was reviewed.

3.1 Transaction Procedure:

According to Lawrence et al., (2002), Transaction Procedures are needed to facilitate consumers' use of Electronic Payment Systems (EPS) and to eliminate their concerns about the security of EPS. From the viewpoint of Hwang et al., (2007), it is necessary to accomplish the requirements related to consumer's security which can be achieved by establishing well-defined EPS procedures. Measuring of transaction procedure involves the usage of the following three factors, namely, Authentication, Modification, and Confirmation. Authentication is the procedure by which the identity of participants is verified through their identity and password

- *Thirupathi Chellapalli, is currently working as an Assistant Professor at Gitam Hyderabad Business School (GHBS), Gitam (Deemed to be University) Hyderabad Campus, Rudraram, Hyderabad, Telangana, India, PIN: 502329, His E-mail Id: thirupathi.chellapalli@gmail.com Mobile: +91 8897259193*
- *Daruri Venkata Srinivas Kumar is currently working as an Assistant Professor at School of Management Studies, University of Hyderabad, Hyderabad, India, 500046. His email id: srinivasdaruri@gmail.com*

before they participate in an e-payment system (Tsiakis and Sthephanides 2005, Hwang et al. 2007). Even though authentication provides a preliminary process that precludes illegal intrusion, it is subjected to risks because of the open nature of Internet authentication which is a visible procedure that is directly related to payment security and thus influences consumers' perception of security and trust (Laudon and Traver 2001, Tsiakis and Stephanides 2005, Kousaridas et al 2008). According to researchers, the modification is the process following which consumers terminate or amend payment amount or method before completion of the ultimate stage of the payment process. This provision would arouse confidence in customers as it would reassure them that in the payment transaction process they have control till the last stage (Laudon and Traver 2001). Confirmation is the process that provides the guarantee of receiving payments to customers (Linck et al. 2006). In this procedure, merchants send an acknowledgment by using mobile phone messages, emails, faxes, etc. According to Romdhane (2005), the provision of acknowledgment information regarding a payment affects consumers' perceptions of security in electronic payment systems (EPS) use.

Research Question: Does transaction procedure has a positive association with perceived security and customers' usage of EPS?

Hypothesis: Transaction Procedure has a positive association with Perceived Security and customers' usage of EPS.

Technical Procedure has also been discussed at length in the prior literature by various researchers such as Link et al. (2006), Hwang et al. (2007), and Kousaridas et al. (2008). The procedures in electronic payment solutions differ from the ones followed in traditional payment procedure because there is a fundamental difference in the transaction infrastructure. Though EPS can overcome the constraints of time and space, which gives EPS an advantageous position over the traditional offline transactions, however, challenges related to the security of the operations remain.

3.2 Technical Protection:

Technical Protections are the foundation of EPS security. A series of specific technical mechanisms are utilized to ensure payment security during the transaction process on the internet (Slyke and Belanger (2003), Linck (2006), Kousaridas et al. 2008). Considering the problem related to consumer trust, Technical Protections are designed to ensure a reduction in risk which has been addressed by Kalakota and Whinstone (1997). For measuring the technical protections, the following three categories have been considered: privacy, integrity, and confidentiality (Friedman et al. 2002, Tsiakis and Sthephanides 2005, Hwang et al. 2007). A privacy protection mechanism can assure 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 ensure that the information provided to merchants during an e-payment process cannot be used by other parties (Slyke and Belanger 2003, Chou et al. 2004). These technical protections can be achieved by certain specific policies. Standardization is the manner in which consumers' information is utilized, stored and securely protected (Pilioura 2001). Some consumers are reluctant to

use EPS because of the fear that there will be a misuse of their personal details which will become available on the internet (Kalakota and Whinstone 1997, Wright 2002). Integrity measures the security of payment information both during and after a payment process (Romdhane 2005). Integrity mechanisms ensure that other parties do not intercept or alter e-payment information (Tsiakis and Sthephanides 2005, Hwang et al. 2007, Kousaridas et al. 2008). This can be achieved via the use of encryption mechanisms including secure sockets layer (SSL) and secure electronic transactions (SET) technologies (Slyke and Belanger 2003, Dahlberg et al. 2008). The typical requirement of consumers is that the amount of payment and other data remain unchanged (Laudon and Traver 2001). This mechanism influences consumers' perceptions of security and trust in (electronic payment systems) EPS use. Ultimately, confidentiality is related to preventing unauthorized people from getting access to personal details of customers because it arouses confidence in EPS. There are a variety of factors that may affect the confidentiality of electronic transactions, including e-payment software, e-payment database, e-payment system platforms and power supply (Kalakota and Whinstone 1997). Additionally, technical protection of establishing authentication of parties, such as the two-factor authentication is also necessary for confidentiality.

Research Question: Does Technical Protection has a positive association with Perceived Security and consumers' usage of EPS?

Hypothesis: Technical Protection has a positive association with Perceived Security and consumers' usage of EPS.

3.3 Perceived Security:

Several factors influence the security of e-payment transactions such as systems factors which include technical infrastructure and implementation as stated by Laudon and Traver (2001) and transaction factors which include securing payment through specific rules as stated by Hwang (2007) and Lim – (2008). Peha and Khamitov (2004) referred to legal factors, that is, designing a framework of an electronic transaction based on law. By reviewing the existing security techniques for EPS, including encryption and authentication technique, Slyke and Belanger (2003) concluded that an e-payment system will be considered secured only if it protects consumer's personal details and prevent deceptive activities. On the basis of the three factors—availability, accessibility, and comprehensibility—the security measures are measured. Availability refers to the information supporting e-payment system usage by consumers (Mukherjee and Nath 2003). Consumers require knowledge regarding the varied options and functions that are provided by EPS. Inadequate statements about EPS usage guidelines can act as an interference for customers (Lim 2008). Therefore, description about usage of e-payment system must be in lucid language focusing on technical details and functionality, namely, functions and options within an e-payment, explanations as to how to use an e-payment function, and advice on how to prevent details on e-payment systems (Miyazaki and Fernandez 2000, Tsiakis and Sthephanides 2005, Lim 2008). Along with the information that makes a customer aware about trustworthy and untrustworthy merchants, EPS can provide other relevant information. For instance, a reputation system

can promote usage of EPS by customers. Accessibility refers to the convenience with which consumers can locate statements that concern the security aspects of EPS (Wright 2002, Hegarty et al. 2003). No extra effort must be required from the end of the customers to understand security statements. The instructions related to security should be made available either on the e-payment webpage or other linked webpages. It is, therefore, necessary for a well-designed e-payment system to make it easier for customers to learn about security related issues (Cotteleer et al. 2007). Finally, comprehensibility refers to the manner in which security statements are provided to the consumers (Linck et al., 2006). The security statement should be explicit and straightforward enough for an average consumer to comprehend easily. The instructions must also make customers' aware about the transaction process when customers make e-payment (Mukherjee and Nath 2003). Accordingly, an original e-payment system must have the following characteristics: i) the security statement must be precise and all-inclusive; and ii) the security statement must make customers' aware (Hsieh 2001, Cotteleer et al. 2007).

Research Question: Does perceived security have a positive association with consumers' usage of EPS?

Hypothesis: Perceived Security has a positive association with consumers' usage of electronic payment systems.

According to Linck (2006) and Kourasidan (2008), discernment of customers about security related to e-payment is crucial for enhancing EPS usage. Laudon and Traver (2001) argued that in EPS sophisticated processes and methods need to be developed for dealing with security requirements. Lawrence (2002) also suggested that in EPS the refined process interactions can eradicate the fear of customers related to security issues about EPS usage.

4. RESEARCH OBJECTIVES:

- To Study the association among Transaction Procedure and Perceived Security and Electronic Payment Systems (EPS) Usage.
- To Study the association among Technical Protection and Perceived Security and Electronic Payment Systems (EPS) Usage.
- To Study the association between Perceived Security and Electronic Payment Systems (EPS) Usage.

5. RESEARCH HYPOTHESES:

H1: Transaction Procedure has a positive association with consumers' Perceived Security.

H1 (a): Transaction Procedure has a positive association with consumers Electronic Payment Systems (EPS) Usage.

H2: Technical Protection has a positive association with consumers' Perceived Security.

H2 (a): Technical Protection has a positive association with consumers Electronic Payment Systems (EPS) Usage.

H3: Perceived Security has a positive association with consumers Electronic Payment Systems (EPS) Usage.

6. RESEARCH METHODOLOGY:

The present study collected relevant primary data with the help of structured questionnaire from the respondents

(professionals, employees, businessmen, students, etc.) in Hyderabad city, India. The questionnaire was designed to capture the demographic details of the respondents and their opinions on transactional procedures, special protection, and perceived security of EPS.

7. RESEARCH INSTRUMENT:

A structured questionnaire was used to gather information from the respondents. The questionnaire is divided into three main sections. The first section is related to demographic data of the interviewees, and the second section is related to capturing the awareness levels and usage of online payment services, and finally, perceptions (transactional procedure, technical protection, perceived security, increased usage) of respondents towards EPS. The Likert five-point scale ranging from "Strongly Disagree" to "Strongly Agree" was used in this study. The respondents were asked to give their perception of factors on a five-point Likert scale (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree), and a total of 167 usable survey forms were considered for the study. A quantitative study based on the information collected during the inquiry was conducted to empirically validate the identified factors of perceived security, transactional procedure, technical protection, etc., which influenced EPS. The data were analyzed by using SPSS software.

8. RESULTS & DISCUSSIONS:

The mean and standard deviation were calculated for the scores obtained on the parameters related to transaction procedures, technical protection, perceived security, and EPS usage.

8.1 Correlation Analysis

	M	SD	1(TP)	2(TPr)	3(PS)	4(EPSU)
1.Transaction Procedure (TP)	15.84	3.35	1			
2.Technical protection (TPrt)	17.83	3.12	.384**	1		
3.Perceived security (PS)	14.00	2.77	.192*	.561**	1	
4.EPS Usage (EPSU)	6.74	1.65	.266**	.285**	.505**	1

Note: n = 167, **P < 0.01, *P < 0.05, M is the mean and SD is the standard deviation.

Table: 1 Correlation Analysis

Correlation co-efficient (r) between transaction procedure, technical protection, perceived security and EPS usage are presented in the above table. Positive correlation is found between transaction procedure and technical protection (i.e., n = 167, r = 0.384, P < 0.01) which indicates a weak linear relationship. A weak positive relationship is found between transactional procedure and perceived security (n = 167, r = 0.192, P < 0.05) as well as between transaction procedure and EPS usage (n = 167, r = 0.266 P < 0.01). It is also observed from the table that there is a moderate to strong positive relationship between technical protection and perceived security (n = 167, r = 0.561, P < 0.01). The relationship

between technical protection and EPS usage is observed to be weak ($n = 167$, $r = 0.285$, $P < 0.01$). Finally, there is a positive moderate relationship between perceived security and EPS usage ($n = 167$, $r = 0.505$, $P < 0.01$).

8.2 Multiple Linear Regressions:

The coefficient of determination R^2 and F values have been computed to find out the impact of transaction procedure and technical protection on perceived security, and the results are presented in the table below.

	B	SEB	β	t	r
Transaction procedure	-0.02	0.06	-0.03	-0.39	0.19*
Technical protection	0.51	0.06	0.57	8.16**	0.56**
R^2	0.32				
C	5.30				
F	37.67				

Note: Adjusted $R^2 = 0.31$ B = Un Standardized beta coefficient, SEB = Standardized error of beta, β = Standardized beta co-efficient, C = constant, t = t values of beta, SE = Standard errors of the estimate, adjusted $R^2 = 0.31$ and $n = 167$, ** $P < 0.01$, * $P < 0.05$.

Table: 2 Multiple Linear Regressions

It can be observed from the Table 2 that both the predictors (Transaction Procedure and Technical Protection) are considered for determining the impact of transactional procedure and technical protection on perceived security. The combined predictors explained 32% of variance in perceived security, $R^2 = 0.32$ adjusted $R^2 = 0.31$ and $F(1, 166) = 37.67$ ($P < 0.01$). Transactional procedure was not a significant predictor ($\beta = -0.03$, $P > 0.05$). The effect of transaction procedures on consumers' perceived security was not significant, showing that the transaction procedure does not act as an antecedent of consumers' perceived security in EPS. Technical protection was a significant predictor ($\beta = 0.57$, $P < 0.05$) and the effect of technical protection act as an antecedent of consumers' perceived security in EPS. The multiple regression analysis suggests that technical protection is associated with perceived security.

	B	SEB	β	t	r
Transaction procedure	0.10	0.04	0.20	2.76*	0.27**
Technical protection	-0.04	0.05	-0.08	-0.911	0.29**
Perceived security	0.30	0.05	0.51	6.39*	0.51**
R^2	0.29				
C	1.69				
F	22.01				

Note: Adjusted $R^2 = 0.28$ B = Un Standardized beta coefficient, SEB = Standardized error of beta, β = Standardized beta coefficients, C = constant, t = t values of beta, SE = Standard errors of the estimate, adjusted $R^2 = 0.28$ and $n = 167$, ** $P < 0.01$, * $P < 0.05$.

Table 3: Multiple Linear Regressions

From the above Table, the combined predictors explained 29.1% of the variance in EPS Usage. $R^2 = 0.29$, adjusted $R^2 = 0.28$ $F(1, 166) = 27.01$ $P < 0.51$, among the transaction procedure was more significant predictor ($\beta = 0.20$, $P < 0.05$). The effect of transaction procedure on consumers' EPS usage was significant, demonstrating that the transaction procedure acts as an antecedent of consumers' EPS usage, whereas technical protection was not a significant predictor ($\beta = -0.08$, $P > 0.05$). The effect of technical protection on consumers' EPS usage was not significant, demonstrating that technical protection does not act as an antecedent of consumers' EPS usage, whereas perceived security was the most significant predictor ($\beta = 0.51$, $P < 0.05$). The impact of perceived security on consumers' usage of EPS was significant, demonstrating that perceived security act as an antecedent of consumers' EPS usage.

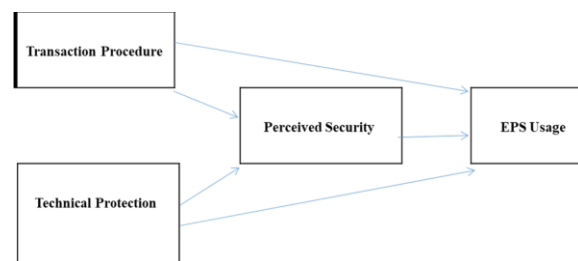


Fig: 1. Research Model of Perceived Security in E- Banking Payment Systems Usage

Hypotheses	Results
H1: Transaction Procedure has a Positive Association with Consumers' Perceived Security.	Not Supported
H1 (a): Transaction Procedure has a Positive Association with Consumers Electronic Payment Systems (EPS) Usage.	Supported
H2: Technical Protection has a positive association with consumers' Perceived Security.	Supported
H2 (a): Technical Protection has a Positive Association with Consumers Electronic Payment Systems (EPS) Usage.	Not Supported
H3: Perceived Security has a Positive Association with Consumers Electronic Payment Systems (EPS) Usage.	Supported

Table: 3 Results of Hypothesis Testing

9. IMPLICATIONS:

The study would give insights into the various aspects of the relationship between customer perceived security and usage of EPS. As the role of technology further increases in various aspects of banking like the adoption of smartphones, cardless ATM transactions, etc., it is quite important to understand the concerns of customers towards various security issues related to electronic banking. Innovations in Self-Service Technologies (SSTs) are bound to change the face of the banking industry. As the country progresses towards more inclusive economy, banking firms are facing a huge challenge in understanding the needs and concerns of various customer segments and these companies address the challenges involved in the adoption of technologies by the customers.

10. LIMITATIONS OF THE STUDY:

1. The study constituted a sample of 167 respondents from Hyderabad city.
2. The study captured the responses of the interviewees related to the perceived security in electronic banking and the reasons behind referring to a particular kind of electronic banking facility that is not captured.
3. The respondents included retail banking customers only.

11. CONCLUSION:

Security is the prime concern of clients who rely on various modes of electronic banking with the developments in IT and telecommunications, various innovative modes of payments are being introduced by the banking industry. Electronic banking offers convenience to the customers regarding saving time and energy which at the same time benefits banks. Given enormous cost savings associated with the introduction of electronic banking based on the proliferation of information communication and technology which is coupled with the explosion in smartphone usage and the advent of online or electronic retailing, the electronic payment mechanisms are bound to play a pivotal role in the development of the economy. However, along with the increase in usage of electronic banking, frauds like phishing, stealing of passwords, cloning of cards, etc. are also on the rise. Electronic fraud is one of the biggest challenges bankers need to address. In this context, it is quite necessary to understand the perceptions of customers related to security issues in electronic banking. Once these matters have been identified, it becomes easier for the banks and financial institutions to address these problems and find solutions as well as provide assurance to the customers using electronic banking. Electronic banking offers the convenience of banking anywhere and anytime; it has the potential to make banking affordable and accessible across various sections of the society.

12 REFERENCES

- [1] Chellapalli, T., & Srinivas Kumar, D. V. (2016). Electronic Payment Systems: Role of Demographics. *SCMS Journal of Indian Management*, 41–52.
- [2] Anderson, J.N., Weir, C.S., Jack, M.A., 2006. On the role of metaphor and language in the design of third party payments in e-banking: Usability and Quality. *International Journal of Human-Computer Studies*, 64(8), 770-784.
- [3] Benson, K., 2008. *Commercial Banks in India: Growth, Challenges, and Strategies*. New Century Publications, New Delhi.
- [4] Bhasin, N., 2006. *Banking Development in India 1947 to 2007: Growth, Reforms & Outlook*. New Century Publications, New Delhi.
- [5] Chou, Y., Lee, C., Chung, J., 2004. Understanding m-commerce payment systems through the analytic hierarchy process. *Journal of Business Research*, 57(12), 1423-1430.
- [6] Devika, M.V., Latasri, O.T.V., 2011. Study on customer satisfaction of electronic payment system. *Cauvery Research Journal*, 5(1-2), 29-34.
- [7] Gurusamy S, 2001. *Banking in the New Millennium: Issues, Challenges & Strategies*. Kanishka Publishers & Distributors, New Delhi.
- [8] Herzberg, A., 2003. *Payments and banking with mobile personal devices*. *Communications of the ACM*, 46(5), 53-58.
- [9] Hsieh, C.T., 2001. E-commerce payment systems: critical issues and management strategies. *Human Systems Management*, 20(2), 131-138.
- [10] Kim, C., Tao, W., Shin, N., Kim, K.S., 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1), 84-95.
- [11] Lal, D.R., Saluja, D.R., 2012. E-Banking: The Indian Scenario. *Asia Pacific Journal of Marketing & Management Review*, 1(4), 16-25.
- [12] Lim, A.S., 2008. Inter-consortia battles in mobile payments standardization. *Electronic Commerce Research and Applications*, 7(2), 202-213.
- [13] Özkan, S., Bindusara, G., Hackney, R., 2010. Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis. *Journal of Enterprise Information Management*, 23(3), 305-325.
- [14] Reserve Bank of India, 2009. *Report on Trend and Progress of Banking in India*. RBI, Mumbai.
- [15] Singh, S., 2009. The emergence of payment systems in the age of electronic commerce: The state of the art. *First Asian Himalayas International Conference on the Internet* (pp. 1-18). IEEE.
- [16] Sharma, H., 2011. Bankers' Perspective on e-banking. *Global Journal of Research in Management*, 1(1), 71-84.
- [17] Uppal, R.K., 2011. E-Age Technology-New Face of Indian Banking Industry: Emerging Challenges and New Potentials. *Journal of Social and Development Sciences*, 1(3), 115-129.
- [18] Uppal, R.K., 2011. E-Delivery Channels in Banks-A Fresh Outlook. *Researchers World*, 2(1), 180-191.
- [19] Uppal, R.K., Kaur, R., 2007. *Banking in the New Millennium-Issues, Challenges, and Strategies*. Mahamaya Publishing House, New Delhi. J.S. Bridle, "Probabilistic Interpretation of Feedforward Classification Network Outputs, with Relationships to Statistical Pattern Recognition," *Neurocomputing—Algorithms, Architectures and Applications*, F. Fogelman-Soulie and J. Hérault, eds., NATO ASI Series F68, Berlin: Springer-Verlag, pp. 227-236, 1989. (Book style with paper title and editor)