Fintech innovations in E-payments: Privacy and security in cybercrime threats

K. P. Ramesh | R. Amudha | K. Prasob | K. S. Kanna

Abstract The digitalization challenges in the e-commerce world provide ample opportunities and advantages for the corporates, financial institutions and the consumers but also have posed several threats in the form of financial thefts and cyber frauds. The Fintech innovations have brought in effective solutions for many fraud detections and poised to have a controlled safety and security systems in handling the financial and other commercial transactions, most specifically in the fund transfers and other payment processes in the Electronic Payments Systems (EPS) in the current era. Absence of security culture is vulnerable to incur heavy and unaffordable costs to the service provider’s organization pertaining to financial frauds, cybercrime threats, identity larceny, illegal procedures, loss of consumer confidence, etc. Hence, in today’s robust e-commerce scenario the vitality of Fintech Innovative solutions, Security enabled systems, ensuring Safety and Privacy of Information of the customers are of prominence. This research study analyses the Fintech Innovative solutions, on the security, safety and privacy of customer’s information on effective Electronic Payment Systems (EPS) and the legal safety assurance on cybercrimes.

Keywords: fintech innovations, perceived safety, perceived privacy, EPS protection and usage, cybercrime safety applications

1. Introduction

The challenges in digitalization and consumer behavior pose the need for exploring new and innovative technologies for creating robust electronic platforms either for the purpose of complying or for competing. Payments’ security is becoming more imperative due to increasing card fraud losses and data breaches that result in direct and indirect losses for the affected financial institutions. Security controls employed in electronic payment systems are expected to be more vigorous and may frustrate users in payment handling applications. Security systems are more than an add-on requirement; they need to be implemented as a culture both as a mindset and as a mode of operation across organizations to mitigate financial fraud. The absence of security culture leads to uncertainty and ultimately results in security incidents that are vulnerable to heavy and unaffordable costs. Any innovations have to be initiated in a secured environment rather than an unsecured innovative system. Hence, failure to secure sensitive information by organizations can cause severe damage to the service provider’s organization pertaining to financial deceptions, identity larceny, illegal policy procedures, loss of consumer confidence, etc. In today’s robust e-commerce scenario, the vitality of fintech innovative solutions, security enabled systems, and ensuring the safety and privacy of information of customers are prominent.

2. Literature Review

Lee et al. (2001) stated that the extensive use of telecom networks and the increase in commercialization in the current dynamic e-commerce world have provided innumerable advantages over the traditional system for financial transactions with regard to speed, openness, anonymity and global accessibility, improving the individual user’s quality of life. Boosting the popularity of electronic payments ultimately enhanced the competitive edge of companies that have adopted technology innovations to maintain enhanced business relationships due to secured EPS (Vladimir Zwass 1996). Ensuring that these systems are effectively applied across Turkish and US university students across countries (Lightner et al., 2002). The edifice of electronic commerce (EC) is EPS, and with its increase in volumes of EC, EPS has become increasingly vital for businesses and individual users (Linck et al., 2006) has stated that for any advanced electronic commerce utilizing businesses, EPS is considered the most crucial determinant for its success and sustenance. In the scenario of EPS advancements in the past decade, security and privacy issues are of predominant concern and continue (Shon and Swatman 1998). Security is the ‘set of procedures, mechanisms and computer programming, authenticating the sources of information and to guarantee the
reliability of the data, to abstain leading to a hardship of economic data resources’ (Tsiakis and Sthepanides 2005), whereas privacy is ‘the form of confidence held on the business partners based on the reliability and integrity’ vital in transactional relationships, especially those involving high risk, specifically in online transactions (Liao and Chen 2011; Reicheld and Schefter 2000). Internet connectivity allows hackers to connect to countless other computers and transmit information, messages, and data, which unfortunately also allows these cyber criminals to communicate with other criminals and with their victims, a threat to malicious stealing of data (Smitha and Ammar 2012).

3. Vitality of Fintech Innovations and Security

In the present technological advancements, both innovation and security are equally vital. It is a known fact that our own smartphones have been exposed to the greatest privacy risk. In this context, an increasing number of businesses need to deploy EPS in all their commercial transactions to meet increasing demands and, due to government pressures, to depend on a speedy and secured EPS for their clients/customers. All effective applications and prudent implementation processes of the EPS to the dismal resulted in several hacking crimes causing financial losses for the companies. The stringent fraud detection processes resulting from the FinTech procedures culminate as the solution provider for effective EPS implementation. Emerging developments in technology hamper the growth of the m-payments industry as the market becomes fragmented (Lim 2008).

4. Safety and Privacy issues in EPS

The individual user’s quality of life has improved to a larger extent due to the popularity of fintech innovations, thereby enhancing the competitive edge of the companies that have adopted at the right time. Although businesses have thrived due to innovative fintech advancements and improved EPS applications, the safety, security and privacy issues of the information shared electronically are still a matter of concern, preventing integrity and trust in the companies implementing their business processes. This trust, safety and privacy issue has been a challenge preventing individuals from engaging in e-commerce transactions and fund transmittances. Informed consent is an important human value that integrates online interactions wherein just-in-time interventions are employed to meet their goals (Friedman et al., 2002). Hence, the economic growth of the country and the business growth of companies demands additional safety and privacy of information in fintech innovations for effective and efficient EPS implementations of companies for viable and trustworthy EPS usage from the customers’ viewpoint.

5. Cybersecurity applications and protecting laws

The primary stakes of cybersecurity against cyber threats in need are as follows:

- Network security solutions are designed to identify and block cyber-attacks, especially in financial transactions.
- Cloud Security: the digital transformation era to incorporate cloud-based tools and services as a part of the business infrastructure.
- Endpoint Security: high need to protect devices such as workstations and servers from malicious cyberattacks
- IoT Security: securing Internet devices and the networks they’re connected to from threats and breaches by protecting, identifying, and monitoring risks
- Application Security: developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
- Zero Trust: a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration

Therefore, perceived security was found to be an essential variable in understanding consumer behavior and trust in e-payments (Chellappa and Pavlov 2002).

6. Objectives of the study

- To comprehend the antecedents of the perceived safety and privacy issues on EPS and cyber threat protective usage
- Examining the privacy and security challenges to eliminating financial fraud through fintech procedures in the EPS from an individual user’s viewpoint
- Identify individual user’s personal experience of Electronic Payment Systems (EPS) and cybercrime protection.

7. Statement of the problem

The innovative inclusions of electronic payment systems (EPS) have improved individual users’ quality of life in terms of speed, accuracy, security, privacy and ease of payments for online fund transactions. The outcomes of innovative technology with privacy and security using EPS have been a long-term debate, and finding solutions to resolve these issues continues to be a challenge. The study analyses the impact on the privacy and security risk in the process of eliminating financial frauds
ensuring secured EPS. Data collected from 296 sample respondents indicate that both perceived safety and privacy have a significant influence on EPS innovation and usage. Trust and confidence models are used interchangeably, whether supportive or skeptical (Earle 2009).

Electronic commerce has amplified the competitive internet markets overpowering traditional markets due to several novel EPS brands, such as paypals, credit cards, debit cards, prepaid wallets, electronic cheques or e-payments, an imperative requirement to execute electronic fund transfers and other e-commerce transactions. Hence, there is a need for advanced protections to address security, privacy and trust issues through secured EPS and cybercrime protection.

8. Research Design

The lack of perceived security and privacy issues certainly erodes the willingness and trust to use EPS by individual users (Linck et al 2006; Mukherjee and Nath 2003). The conceptual model has been developed and tested based on the determinants of the study, such as the fund transaction process, FinTech application procedures, security-linked applications and the detection of fraud processes that affect perceived safety and perceived privacy in the output of effective EPS protection and usage (Figure 1).

9. Hypotheses Tested

H1: The fund transaction process has a substantial effect on the perceived safety and perceived privacy in EPS protection and usage.

H2: FinTech procedures have a major effect on the perceived safety and perceived privacy in EPS protection and usage.

H3: Security applications have a substantial effect on the perceived safety and perceived privacy in EPS protection and usage.

H4: The detection of fraud in cybercrime has a substantial effect on the perceived safety and perceived privacy in EPS protection and usage.

H5: Perceived safety has a substantial influence on EPS protection and usage.

H6: Perceived privacy has a substantial influence on EPS protection and usage.

10. Analytical discussions

10.1 The composite reliability (CR) and Cronbach’s alpha are tested for the selected determinants of EPS

From Table 1, the average variance, composite reliability and Cronbach’s alpha were captured from the data analysis. According to Hair, Anderson & Black (2007), values above 0.50 are acceptable for the average variance. Since all the values of average variance are larger than 0.5, convergent validity is present for all the variables. The composite reliability (CR) of each variable accepts values above 0.70. The composite reliability (CR) and Cronbach’s alpha, as shown in Table 1, have values greater than the suggested cutoff value of 0.70, indicating that the reliability of all variables is acceptable.

10.2 Structural equation model analysis of the EPS

The structural equation model was then applied to represent the hypothesis generated to test the goodness of fit (Figure 2).

### Table 1 Cronbach’s alpha on the determinants of EPS.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cronbach’s Alpha (α)</td>
<td>0.85</td>
<td>0.88</td>
<td>0.92</td>
<td>0.89</td>
<td>0.90</td>
<td>0.85</td>
<td>0.92</td>
</tr>
<tr>
<td>Aver Var</td>
<td>0.56</td>
<td>0.64</td>
<td>0.68</td>
<td>0.72</td>
<td>0.66</td>
<td>0.69</td>
<td>0.82</td>
</tr>
<tr>
<td>CR</td>
<td>0.85</td>
<td>0.87</td>
<td>0.92</td>
<td>0.89</td>
<td>0.90</td>
<td>0.86</td>
<td>0.92</td>
</tr>
</tbody>
</table>
10.3 Model Fit Analytical Results

The CFA (Confirmatory Factor Analysis) indicates a good fit of the measures ($x^2=988.60$, df=2.612; CFI=.907; IFI=0.91 & RMSEA=0.075), and all the values met the threshold requirements. The measures of the varimax eigenvalues that show values greater than one are accepted, and the results exhibit discriminant validity. Subsequently, the structural equation model was tested to assess the inclusive goodness of model fit. The results indicate that the model fits the data and is within the thresholds ($x^2=1069.015$, p<.001, CMIN=2.766; CFI=0.91; IFI=0.898; RMSEA=0.078).

11. Findings

The perceived safety and privacy of EPS users provides a deeper understanding of all the constructs developed and shows that these two major constructs have a positive and significant effect on EPS usage. When the underlying constructs impacting the two major variables assure security and convincing, they are more willing to adopt EPS fund transfers and transactions. The results have also shown that the fintech procedures applied have been a strong determinant of both perceived safety and privacy factors, with an increasing number of users trusting the EPS systems simultaneously contributing to the growth of businesses.

Consumers increasingly engaging EPS increase the success rate of businesses but are influenced by perceived safety and perceived privacy. Understanding the implications of the influencing factors determines the enhanced use of EPS. This insists on delivering maximum possible fraud detection in the application of Fintech procedures and the adequacy and reliability of security applications for protection in the fund transfer process. EPS ensures the safety of the individual user’s personal details (name identity, contact number, address of communication, credit card details, and bank account details), which are kept secure enough, and the fund transfers are speedy, easy, reliable, trustworthy and safe. The results have shown that cybercrime fraud detection and protection are prominent determinants of fund transfer trust and security. It is essential for the companies to have a close monitoring system and stringent surveillance on any dissatisfaction of the consumers in the EPS handling systems. Stringent cyber threat laws enforced strictly shall be the ultimate solution.

12. Conclusions

The present study has initiated a research model to test the validity of the pertinent determinants identified for the study, which are perceived safety and perceived privacy affecting the use of the EPS systems administered by the companies. The results of the study have been authenticated through the data analysis and findings that the ‘Fund transfer process’ relies on the novel ‘Fintech procedures’ ensuring ‘fraud prevention’ and ‘secured applications’ impacting the primary determinants, i.e., perceived safety and privacy, toward the success rate of EPS usage.

The study observes a noteworthy relationship between fintech procedures and perceived safety and privacy in e-payment system usage because consumers need not focus on the complexity and time-consuming fintech procedures; they only give importance to convenience and protective EPS usage. Although the findings cannot be generalized to a larger population, the study has effectively brought out the results of the two predictor variables (perceived safety and privacy) relating to the use of EPS in business transactions, most specifically protection against cybercrime threats. Ultimately, the question arises as to which is more important, whether innovation or security and safety systems, and the solution that emanates from the success of any innovation is based on the safety and security of the systems usage. Web-driven electronic
commerce is redefined by the dynamics of Internet and fintech innovative solutions, necessitating a look forward to the role of EPS as a pragmatic upgrade to safety, security and privacy systems.

**Ethical considerations**

Not applicable.

**Declaration of interest**

The authors declare no conflicts of interest.

**Funding**

This research did not receive any financial support.

**References**


