Educational Administration: Theory and Practice
2024, 30(11), 3186-3190
ISSN: 2148-2403
https://kuey.net/ **Research Article**

Factors Affecting Security of Electronic Payment Systems

Pardeep Kumar[1*], Rajender Singh[2]

[1*,2]Research Scholar, and Associate Professor, Computer Science and Engineering, Raffles University Neemrana, pardeepkhatana4@gmail.com, raj21engg@gmail.com

Citation: Kumar, Pardeep and Singh, Rajinder (2024). Factors affecting security of electronic payment systems, *Educational Administration: Theory and Practice*, 30(11) 3186-3190
Doi: 10.53555/kuey.v30i11.11366

ARTICLE INFO

ABSTRACT

The high rate of development of electronic payment systems (EPS) has raised the issues of security and safety of users. This paper discusses the issues that influence the security of electronic payment system as viewed by users. A structured questionnaire based on the use of Google Forms was used to gather primary data consisting of 386 respondents. The questionnaire was able to capture five major factors which included technological factor, regulatory factor, human factor, security and trust factor, and user intention factor. The answers were noted using five-point Likert scale. To define the underlying factor structure, exploratory factor analysis was used. The constructs' reliability and validity were evaluated by the address of standard measures. Confirmatory factor analysis was then undertaken on the results as a measure of model validation and model fit. The findings validated the fact that all the five factors have significant impacts on the perceived security of the electronic payment systems. Regulatory guidelines, technological controls and user awareness were identified to have a significant contribution in mitigating security risks. The issue of security and trust became a crucial connection between system characteristics and intent of the user. The results can be valuable to banks, payment service providers and regulators. Payment system security can be strengthened by enhancing the use of technology, better enforcement of regulations and increasing awareness of the users. The research also provides a model of validated measurements that can be implemented in future research related to the field of digital payment security.

Keywords: EPS, Security and Safety, Technological, Human, Intention.

1.1 Introduction

Electronic payment systems have sparked a revolution in the contemporary commercial world as they are convenient and fast. The online banking and online payment systems have become more vulnerable to attacks through mobile payment access that has also led to exposure to security threats, including phishing malware identity theft and data breach. The studies indicate that a blend of technological protection regulatory controls with human behavior affects the issue of payment security (Hassan et al. 2020; Dewi et al. 2023). Technical risks are minimized with strong encryption authentication tokenization, and fraud detection tools, whereas weak system design and old software make the system more vulnerable (Galhotra et al. 2021; Zhang et al. 2023). There exist regulatory frameworks like PSD2 PCI DSS and central bank instructions that enhance trust and compliance but have weaknesses in enforcement which undermine protection (Arner et al. 2020 European Commission 2022). Awareness safe practices among the users and trust perceptions also contribute significantly to the prevention of fraud and the formation of secure usage intentions (Varalakshmi et al. 2024; Al Adwan et al. 2025). These aspects need to be understood to further secure payment and invest in sustainable digital financial systems.

2.1 Literature Review

The use of online technologies has transformed the financial transactions and made the use of electronic payment systems indispensable in the contemporary business. Online banking contactless cards and crypto platforms in the form of mobile wallets are fast and convenient across the globe. Their fast adoption has also augmented the security threats like phishing malware and security breach that are frequently aggravated by user carelessness and lack of awareness (Dewi Ujianto and Rianto 2023). Education and safe practices among

users are useful to avoid fraud and identity theft and enhance system resilience (Varalakshmi Anusuyaa and Baheti 2024). Sustainability of the systems need to be given due considerations (Santibanez et al., 2023). When institutions understand these factors, they enable the institutions regulators and users to build risk and reduce risk to benefit a sustainable digital payment ecosystem. Kumar and Goyal 2022; Zhang et al. 2023 that real time monitoring machine learning and AI are more effective in fraud detection, but data quality and false alerts are also of concern. The customers are influenced by technology and ease of use (Mishra et al. 2024). The most recent research in India and emerging economies indicates that the old software and embedded controls enhance the attacks and that constant changes to adaptive tools and new-fangled technology are needed to mitigate new attacks (Singh and Sharma 2024; Laxman 2025). Technology has immense potential to enhance financial inclusion (Kandpal et al., 2025). As demonstrated by European Commission 2022, PSD2 and strong customer authentication reduced unauthorized access but there were difficulties in their implementation. In India, the guidelines of RBI 2023 minimized the fraud by introducing controls audit and supervision as mandatory. Recent literature attests that articulate data protection legislations and stringent penalties and regulatory clarity enhance compliance consumer trust and adoption whereas lax or ambiguous regulation erode security (Alshammari, 2023; Singh and Kaur, 2024).

3.1 Research Methodology

The research design employed in this paper was quantitative because it was aimed at establishing and establishing factors impacting the security of electronic payment systems. The structured online questionnaire developed with the help of Google Forms was used to gather primary data. Non probability convenience sample of users that had experience in electronic payment systems was used to obtain 386 valid responses. The questionnaire has been formulated based on the previous researches and it contained five variables (as shown in the table 4.1) technological, regulatory, human, security and trust, and user intention measured on a five-point Likert scale between strongly agree (5) and strongly disagree (1). Cronbach alpha was used to test reliability and all the constructs passed acceptable results. The literature and expert review provided content validity whereas factor analysis was used to check construct validity. Principal component analysis with Varimax rotation was used to determine exploratory factors following assessment of sampling adequacy with KMO test, Bartlett test and deletion of low loading items. AMOS was next used to confirmate the factor structure with confirmatory factor analysis and measurement of model fit with standard indices which depicted acceptable outcomes. Cleaned and coded data were analyzed by SPSS on EFA and CFA by AMOS and the results were found to support the proposed factor structure.

4.1 Data Analysis

The electronic payment systems have become a very important pillar of the new commerce because it has made it possible to conduct financial transactions between consumers, businesses and government in a very fast, convenient and borderless manner. These systems are becoming an attractive target to complex cybercrime as the volumes of transactions increase and digital assets become worth more money in question, raising the concern about the confidentiality, integrity, and availability of financial information. In this regard, security is not only a technical necessity but a strategic precondition of maintaining the trust of the users, regulatory adherence, and the sustainability of the digital financial world in the long term.

Table 1. Factors, Reliability, Variables and Factor Loading

Factors, Reliability, Variables and Factor Loading		
Factors & Reliability	**Variables**	**Factor Loading**
Technological Factor (TF) 0.912	Token based features make me feel safe (TF_Q12)	.777
	The app uses tools that help stop fraud (TF_Q11)	.775
	My payment app keeps my data safe (TF_Q07)	.756
	The app updates fix problems in good time (TF_Q10)	.753
	I feel safe from virus and malware when I use payment apps (TF_Q08)	.739
	The app checks like OTP make me feel safe (TF_Q09)	.728
	The login process in my payment app feels safe (TF_Q06)	.722
	I feel safe from replay or hack attempts (TF_Q13)	.714
Regulatory	The system has good checks by the right bodies (RF_Q25)	.787

Factor (RF) 0.906	Staff who manage payment systems have good skills (RF_Q27)	.776
	I feel my data rights are protected (RF_Q23)	.761
	Banks follow the needed safety rules (RF_Q22)	.748
	Payment firms follow the rules (RF_Q24)	.744
	The network and systems feel strong (RF_Q26)	.743
	Rules for payment apps feel clear (RF_Q21)	.701
Human Factor (HF) 0.905	I can use digital tools with ease (HF_Q18).	.783
	I avoid careless actions while using payment apps (HF_Q20)	.765
	My friends and family affect my use of payment apps (HF_Q17)	.764
	My earlier experience with payment apps makes me trust them (HF_Q16)	.753
	I feel customer support helps me when needed (HF_Q19)	.746
	I feel the risk of using payment apps is low (HF_Q14)	.743
	I can identify fake links and fake messages (HF_Q15)	.704
Security and Trust Factor (STF) 0.868	I trust the system to stop fraud (STF_Q31).	.810
	I feel my data is safe when I pay online (STF_Q29).	.794
	I trust the payment system (STF_Q30).	.732
	I feel my payments are safe (STF_Q28).	.701
User Intention Factor (UIF) 0.830	I am ready to use digital payments often (UIF_Q32).	.755
	I will try new payment apps when needed (UIF_Q35).	.719
	I choose digital payments over cash (UIF_Q34).	.717
	I plan to keep using digital payments (UIF_Q33).	.704

The findings indicate high and reliable measurement of all factors. The technology regulatory and human factors are extremely reliable and mirror the user confidence in system security controls rules implementation and individual conscience. Security and trust are also demonstrated as measured and verified the confidence in fraud prevention, and safe transactions. Intention of users is good and indicates frequent usage and availability of continued digital payments due to trust and comfort. The acceptable reliability convergent and discriminant validity and good model fit are confirmed by confirmatory factor analysis. In general, the measurement model is good and applicable to further structure analysis

Table 2: Model Validity Measures

Model Validity Measures									
	CR	AVE	MSV	MaxR(H)	F1	F2	F3	F4	F5
TF	0.912	0.564	0.329	0.912	0.751				
RF	0.905	0.576	0.266	0.906	0.392***	0.759			
HF	0.907	0.581	0.266	0.907	0.457***	0.516***	0.762		
STF	0.868	0.623	0.38	0.87	0.496***	0.509***	0.477***	0.789	
UIF	0.832	0.554	0.38	0.84	0.574***	0.502***	0.477***	0.616***	0.744

The measurement model shows strong reliability and validity across the five factors TF, RF, HF, STF and UIF. Composite reliability values range from 0.832 to 0.912 and exceed the accepted threshold which confirms internal consistency. Average variance extracted values are all above 0.50 ranging from 0.554 to 0.623 which supports convergent validity (Hair et al. 2019). Discriminant validity is confirmed as the maximum shared variance for each construct is lower than its AVE. Maximum reliability values between 0.84 and 0.912 further support construct reliability. Inter construct correlations are significant at p less than 0.001 with UIF showing moderate to strong relationships with the other factors. Overall, the measurement model is reliable valid and suitable for further structural equation modeling and hypothesis testing.

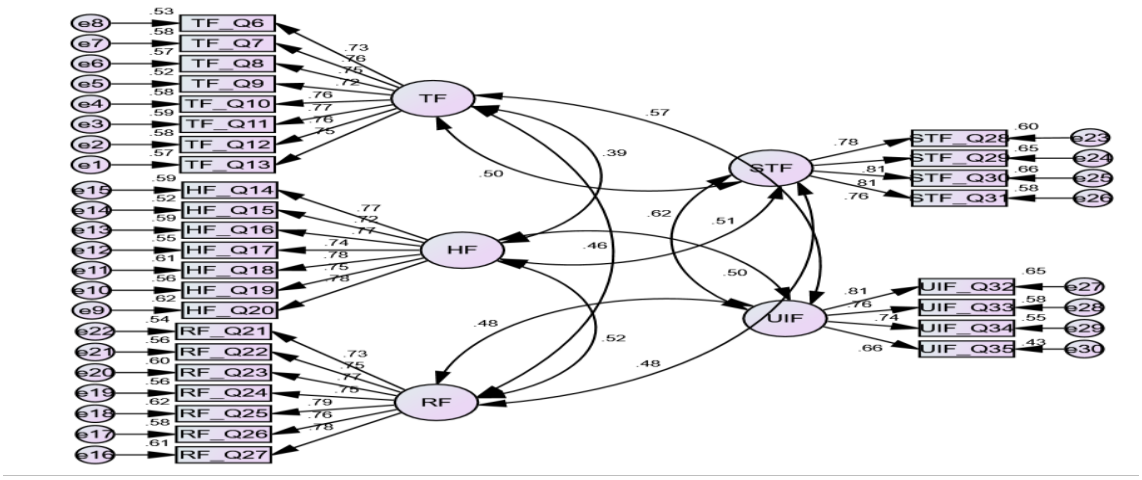

Figure 1: CFA
Sources: primary data

The endogenous constructs in the path diagram of the final structural model of the Factors Affecting the Security of Electronic payment Systems are Safety and Trust Factor (STF), User Intention Factor (UIF) and are influenced by three exogenous factors namely Technical Factor (TF), Human Factor (HF), and Regulatory Factor (RF). The latent variables are quantified by numerous indicators with high standardized loadings (usually around or above 0.70), and the error terms show moderate residual variance, which proves that the observed items are an accurate and valid measure of their corresponding construct. The directional arrows between TF, HF, and RF and STF and UIF reflect the hypothesized causal relationships, whereas the bidirectional arrows between the latent variables reflect the positive covariances of three factors as technical robustness, human related factors, and regulatory support to shape the perceptions of safety/trust and intention to use electronic payment systems in an integrated structural equation modeling framework.

Table 3: CMIN

CMIN					
Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	70	894.222	395	0	2.264

The chi-square statistics indicate that the specified CFA model provides a substantially better fit to the data. In the default measurement model, the chi-square value is 894.222 with 395 degrees of freedom, yielding a chi-square/df ratio of 2.264, which falls within commonly accepted thresholds (often < 3) for an acceptable level of absolute fit in structural equation modeling.

Table 4: Baseline Comparisons

Baseline Comparisons							
Model	NFI	RFI	IFI	TLI	CFI	GFI	RMSEA
Default model	0.875	0.863	0.926	0.918	0.926	0.851	0.057

The base comparison indices and absolute fit indices show that the measuring model has a satisfactory to good degree of fits. All incremental fit indices (NFI = 0.875, IFI = 0.926, TLI = 0.918, CFI = 0.926) are near or above the recommended cutoff value of 0.90, and IFI, TLI and CFI are all greater than 0.92, indicating that the specified model is significantly better than the null (independence) model and that the underlying covariance structure is well covered by it. The goodness of fit factor is low (GPI = 0.851) but slightly lower than the traditional 0.90 standard, but with the other fit measures high, it does not indicate significant model misfit. The value of 0.057 is less than the commonly used upper limit of 0.08 and closer to the more rigorous limit of 0.05 and thus, the model has been fitted to the population covariance matrix closely, with the value indicating only slight residual misfit. These analyses, combined with the chi-square/df ratio that you gave in the prior analysis (2.264), allow concluding that the confirmatory factor analysis model attains an acceptable global fit and can be used in further structural modeling and hypothesis testing in your doctoral research.

5.1 Conclusion

The findings attest to the fact that the five-factor model TF, HF, RF, STF and UIF is a theory based and sound statistically. Exploratory and confirmatory factor analyses exhibit well defined factor structure with strong and

significant loading that follow the convergent validity. The measures of reliability and validity are of accepted standards and a discriminant validity is established. The indices of model fit indicate a well-fitting and acceptable measurement model. The existence of positive relations between all factors testifies that the user awareness regulation via technical controls and trust have a combined impact on the secure and frequent usage of electronic payment systems. This can be used to support additional structural study and measures to enhance payment safety and uptake.

References

1. Al-Adwan, A. S., Yaseen, H., Alkhwaldi, A. F., Jafar, R. M. S., Fauzi, M. A., & Abdullah, A. (2025). Treasure hunting for brands: metaverse marketing gamification effects on purchase intention, WOM, and loyalty. *Journal of Global Marketing*, 1-25.
2. Alshammari, M. (2023). Data protection enforcement challenges. *Information and Computer Security, 31*(4), 587–602.
3. Arner, D. W., Barberis, J., & Buckley, R. P. (2020). The evolution of fintech regulation. *Georgetown Journal of International Law, 51*(2), 1–45.
4. Dewi, A. C., Ujianto, E. I. H., & Rianto, R. (2023). Electronic payment threats and security: A systematic literature review. *Universitas Teknologi Yogyakarta*. Retrieved from https://ejournal.undiksha.ac.id/index.php/janapati/article/down load/76635/29852/233825
5. European Commission. (2022). Payment services regulation PSD2. Official *Journal of the European Union*.
6. Galhotra, A., Jatain, S., Bajaj, S. B., & Jaglan, V. (2021). Mobile payment security issues and solutions. *ICECA Proceedings*.
7. Hair, J. F., Jr., Risher, J. J., Roldán, J. L., & Sarstedt, M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203
8. Hassan, M. A., Shukur, Z., Hasan, M. K., & Al-Khaleefa, A. S. (2020). A review on electronic payments security. *Symmetry, 12*(8), 1344.
9. Kandpal, V., Ozili, P. K., Jeyanthi, P. M., Ranjan, D., & Chandra, D. (2025). Digital Finance and Metaverse in Banking: Decoding a Virtual Reality towards Financial Inclusion and Sustainable Development, *Emerald Publishing Limited*.
10. Kumar, R., & Goyal, S. (2022). Fraud detection technologies in electronic payments. *Journal of Financial Crime, 29*(4), 1231–1245.
11. Laxman, V. (2025). Emerging threats in digital payments. *Financial Crime Review, 9*(1), 22–34.
12. Mishra, D., Agarwal, N., Sharahiley, S., & Kandpal, V. (2024). Digital financial literacy and its impact on financial decision-making of women: Evidence from India. *Journal of Risk and Financial Management, 17*(10), 468.
13. Santibanez Gonzalez, E. D., Kandpal, V., Machado, M., Martens, M. L., & Majumdar, S. (2023). A bibliometric analysis of circular economies through sustainable smart cities. *Sustainability, 15*(22), 15892.
14. Singh, A., & Sharma, R. (2024). Mobile payment vulnerabilities in India. *IJISAE, 12*(2), 45–58.
15. Singh, S., & Kaur, P. (2024). Regulatory impact on digital payments. *Asian Journal of Law and Economics, 15*(1), 55–70.
16. Soundararajan, B. (2021). Challenges and checkpoints of payment systems security. *Journal of Software Engineering and Simulation, 7*(9), 46–53. Retrieved from https://www.questjournals.org/jses/papers/Vol7-issue-9/07094653.pdf
17. Varalakshmi, D., Anusuyaa, S., & Baheti, A. (2024). Cyber security in digital payments: An empirical study. *Asian Journal of Management and Commerce, 5*(1), 305–310. https://doi.org/10.22271/27084515.2024.v5.i1d.274
18. Zhang, Y., Chen, J., & Liu, W. (2023). AI based fraud detection in payments. *Expert Systems with Applications, 213*, 118843.