

SECURITY AND FRAUD PREVENTION IN ELECTRONIC PAYMENT SYSTEMS: UNDERSTANDING USER BEHAVIOUR

SINTHIYA

RESEARCH SCHOLAR / ASSISTANT PROFESSOR, UNIVERSITY SCHOOL OF MANAGEMENT STUDIES, GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI, INDIA, EMAIL: sinthiya.091286@gmail.com

PROF. A. K. SAINI

PROFESSOR, UNIVERSITY SCHOOL OF MANAGEMENT STUDIES, GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI, INDIA, EMAIL: aksaini1960@gmail.com

Abstract

As economies worldwide embrace digital transformation, Electronic Payment Systems (EPS) have become central to financial inclusion, convenience, and the transition toward a cashless society. However, the rapid expansion of EPS also brings growing concerns over security vulnerabilities and sophisticated fraud tactics. This review explores emerging technologies and threats in EPS, analyzing their implications for fraud detection, consumer protection, and regulatory compliance. Drawing from global and Indian contexts, the study reviews key themes including financial inclusion, digital literacy, payment evolution, cashless economy, fraud detection, and the role of security technologies such as biometrics, AI-based monitoring, and tokenization. A conceptual framework is proposed that emphasizes regulatory compliance as the foundation for building a secure and inclusive payment infrastructure. By synthesizing insights across technology, policy, and user behavior, this review contributes a holistic understanding of the EPS landscape and offers direction for future innovation and governance. The findings have practical relevance for policymakers, fintech developers, financial institutions, and educators promoting secure digital financial ecosystems.

Keywords- Electronic payments systems; technology; security; fraud prevention; literature review

1. INTRODUCTION

Lately, Electronic Payment Systems (EPS) have significantly transformed the way individuals and institutions conduct financial transactions (Liu et al., 2025). As the world steadily moves towards a cashless economy, EPS have emerged as pivotal tools for financial inclusion, enhancing convenience, efficiency, and transparency in both developed and developing economies (Rajaguru, 2024). From mobile wallets and internet banking to contactless cards and Unified Payments Interface (UPI) platforms, the evolution of digital payment mechanisms has redefined financial access and participation. The money implemented by these systems is purely digital, which enables rapid and transparent transactions, which reduces costs and increases traceability. Widespread proliferation of mobile payments and e-wallets (like Paytm, Google Pay, M-Pesa etc) suggest people are getting increasingly confident about adopting simple, secure and fast alternatives (Bajwa et al., 2025). Online banking is also gaining popularity with digital banks at the forefront, offering 24-hour account access and digital banking platform, replacing the need for conventional banks. Electronic Payment Systems (EPS) refer to digital platforms and infrastructures that enable the electronic transfer of money between individuals or institutions without the need for notes, coins, cash or cheques (Oney et al., 2017). These are systems such as mobile wallets, web-bases banking systems, QR-Code apps, Point-of-Sale terminals, and contactless options. EPS are designed to become more and more common, as they are very profitable when handled correctly (Liébana-Cabanillas et al., 2024). Security in EPS includes all protective measures and protocols for safeguarding data like integrity, confidentiality and accessibility during financial exchanges. This encompasses encrypted protocols, multi-factor authentication, biometric check, and end-to-end transaction monitoring (Zaffar et al., 2024). Fraud prevention has both proactive and reactive components and these components refer to an organisation's ability to identify, prevent and react to unauthorized or malicious actions such as identity theft, credit card theft, and such related to the same but not limited to identity theft, phishing, card skimming, or other types of fraud (El Hlouli et al., 2023). Related concepts include financial inclusion (aimed at ensuring affordable access to formal financial services for all, particularly the unbanked) and digital literacy (described as the ability of individuals to use digital technologies and platforms capably and securely). All these are strongly linked with the security and adequacy of the modern electronic payment system (Zaffar et al., 2024).

World Bank, and International Monetary Fund reports stress the important role of inclusive digital finance and recommended the establishment of sound regulatory frameworks to reduce the risk of fraud, especially for cross-border transfers (Zhao et al., 2019). To promote consumer awareness and ensure secured conduct of business by financial service providers, the Reserve Bank of India (RBI) in India has provided various guidelines and advisories. Despite these developments, a critical gap remains in integrating insights across technology, regulation, user behavior, and developmental goals. Specifically, limited attention has been paid to how these elements collectively support sustainable development, SDG 9, which emphasizes innovation and resilient infrastructure (Alghamdi et al., 2024). In view of the above background, this investigation marks two main goals. The first objective requires a critical assessment of emerging technologies and threats to Electronic Payment Systems, especially of their implications for the security, fraud prevention, and financial inclusion. The second objective is the conceptual framework supporting relationships between security technologies, digital literacy and regulatory compliance; enabling the implementation of a secure and inclusive digital payment infrastructure supporting SDG-9 (Industry, Innovation and Infrastructure). Together the objectives are aimed to fill up previous gaps in the literature and to give a thorough impression on current developments in the EPS landscape.

This analysis results in a conceptual model that puts regulatory compliance at the core of the secure EPS ecosystem supported by the pillars of security technology, financial inclusion and digital literacy. When designed and implemented well, these effective policies provide the components for the delivery of sustainable and safe financial infrastructure; directly contributing to the success of SDG-9. The framework emphasizes that security and fraud prevention are not isolated challenges but are interdependent with broader goals of digital transformation and social equity.

The implications of this review are manifold. For policymakers, the findings highlight the need to create integrated and forward-looking regulatory environments that encourage innovation while safeguarding public interest. For financial institutions and fintech startups, investing in scalable and user-centric security solutions becomes both a business imperative and a social responsibility. For educators, NGOs, and digital literacy advocates, the study underscores the importance of equipping users particularly from underserved communities with the knowledge and skills to navigate EPS safely. And for researchers and technologists, the paper points toward future opportunities to explore context-sensitive solutions that balance innovation with risk mitigation.

The remainder of this article is organized as follows. We first outline the review question, eligibility criteria, and search strategy, then describe the screening and data extraction processes. We next synthesize the included evidence, highlighting major themes and gaps. We close with a discussion of implications, limitations of the evidence base, and recommendations for future work.

2. RESEARCH METHODOLOGY

The study's methodology is influenced by Bansal et al. (2024) and Nangia et al. (2024), and it incorporates a rigorous review mechanism that provides for a high level of transparency and replicability. To carry out this review, we followed three steps: (i) identifying information sources, (ii) locating relevant articles, and (iii) screening and reviewing the retrieved records. We initiated data collection using the Web of Science, the most widely used database. Our selection rested on two criteria: (i) these databases are most commonly used by social science researchers, and (ii) inclusion of a mix of database types (citation, publisher, and subject-specific) was necessary.

We began with applying the Boolean- TS= ("electronic payment system*" OR "digital payment*" OR "online payment*" OR "mobile payment*" OR "e-payment*")

AND TS= ("security" OR "cybersecurity" OR "data protection" OR "authentication" OR "encryption" OR "risk management" OR "fraud prevention" OR "fraud detection" OR "financial fraud" OR "cyber fraud" OR "anti-fraud system*" OR "anomaly detection"), on the WoS database and retrieved 601 articles. To select the articles for our systematic literature review, we had the following criteria: (i) articles must be published in journals in subject area business, management, business finance, and economics, in English; (ii) articles must mention EPS or digital/online/mobile/e- payments; and (iii) articles must use the keywords related to risk and fraud in their title or abstract. Articles had to meet all three criteria. Following the criteria (i) we eliminate 480 papers leaving us with 121. After refining criteria (ii) and (iii) we further eliminate 19 papers and did the final analysis on 102 articles (see figure 1 for summary).

Over the past twenty years, systematic reviews have become a standard approach for producing targeted syntheses of prior research (Kable et al., 2012). This method typically prioritizes rigorous appraisal, emphasizing validity and reliability. In the present review, we pursued reliability by adhering to Hart's 1998 procedural guidance for conducting literature reviews Hart (1998). Two researchers carried out the process, discussing each stage beforehand and comparing outcomes afterward to strengthen inter-rater reliability in the analysis (Seuring & Müller, 2008). To support

validity, articles were selected using established criteria (Hart, 1998), and we benchmarked constructs against those reported in earlier reviews, both within the domain and in adjacent fields (Fagerberg et al., 2018).

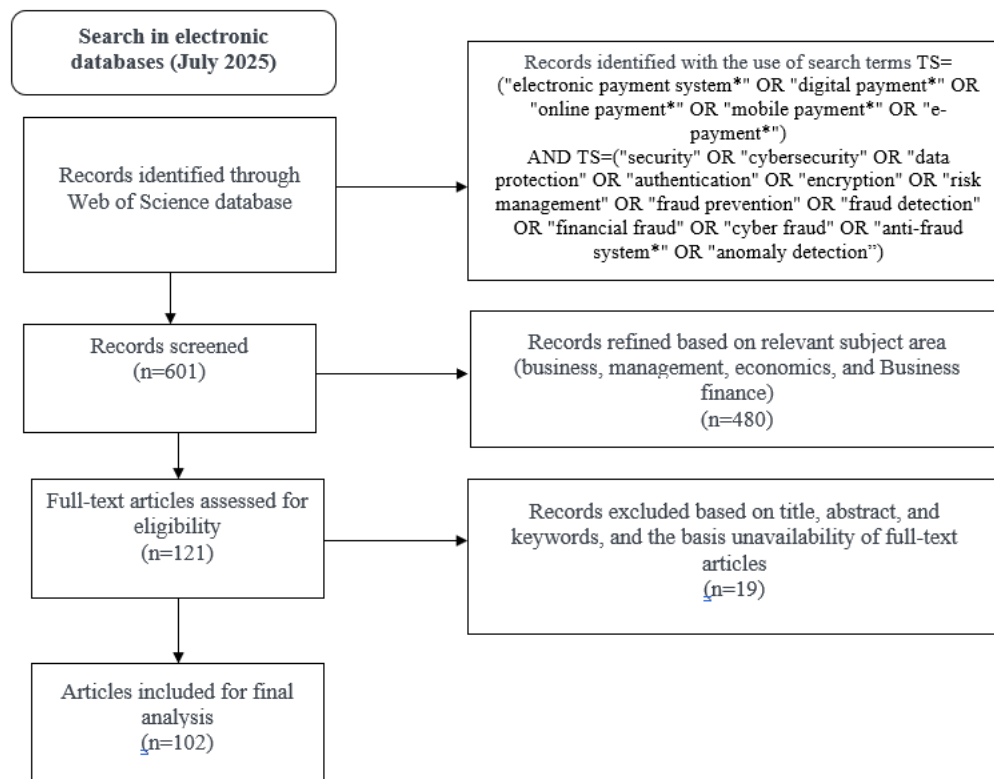


Figure 1 PRISMA diagram

3. RESULTS AND FINDINGS

3.1.1. Thematic findings

Within a thematic map, topics in a conceptual field are arrayed on Cartesian coordinates. The accompanying strategic diagram differentiates themes using two parameters—centrality and density (Cobo et al., 2015). Centrality reflects how extensively a theme connects with other topics, while density gauges the internal cohesion of links within the theme itself (Aparicio et al., 2019). On this basis, the lower-right quadrant (high centrality-low density) corresponds to basic or transversal themes; the upper-left (low centrality-high density) to peripheral or highly self-contained themes; the lower-left (both low density & centrality) to themes that are emerging or waning; and the upper-right (both high centrality & density) to motor themes that drive the area.

Figure 2 showcases a strategic map featuring seven themes distributed across all four quadrants. Prominent topics include payment evolution, financial inclusion, regulatory compliance, and the cashless economy. In that quadrant, internal linkages are relatively weak—suggesting a need for deeper investigation of sub-themes—while connections to other themes have strengthened over time (Rodríguez-Soler et al., 2020). Financial Inclusion, security technologies, and cashless economy are observed as the top three in terms of the degree of centrality. Moreover, the theme, *Financial Inclusion*, comprises keywords such as Fintech integration, rural connectivity, payment infrastructure, micro payments, digital KYC, real-time transfers, subsidy distribution, gender inclusion, financial literacy, cost efficiency, and fintech integration (Azman Ong et al., 2023; Bednarz et al., 2024; Cotugno et al., 2024; Lisana & Handarkho, 2023; Mohd Thas Thaker et al., 2023; Vanini et al., 2023; Xia et al., 2023). Financial inclusion, defined as the provision of affordable, accessible, and appropriate financial services to all individuals, especially the underserved, has emerged as a pivotal element in promoting equitable economic development, reducing poverty, and fostering social empowerment (Bednarz et al., 2024). In rural areas, the combination of fintech, such as mobile money platforms and agent-based models, is particularly significant: it extends the connectivity of financial infrastructure and allows rural areas to join seamlessly within an ecosystem that was previously out of reach for them.

This is attributed to an emerging bottom-up involvement of a strong and interoperable digital payment system Like Unified payments interface in India or M-pesa in Africa, they also open the door for micro-payments and real time

transfers that will enable low-income users to make payments safely, securely and efficiently (Prasetyo et al., 2025). Further in country like India, which has implemented the biometric electronic KYC (e-KYC) systems such as Aadhaar (Wei et al., 2024). Crucially, inclusive finance must also confront gender disparities: women are often systematically lacking in access to financial services. Evidence from Feminist Economics and Development Policy Review shows that this is sometimes because of socio-cultural traditions though other times it's due to limited access to digital services and literal constraints set into law (Laksamana et al., 2023). As Pal et al. (2021) assert, low financial literacy can negate the benefits of access, underscoring the importance of integrating financial education into inclusion strategies. Finally, fintech-driven digitization significantly enhances cost efficiency for service providers, reducing customer acquisition and operating costs by up to 70% (as noted in the Journal of Banking and Finance), thereby making it economically viable to serve low-margin, high-volume segments such as rural and low-income users. In sum, a comprehensive and inclusive approach to financial inclusion anchored in technological innovation, rural outreach, payment modernization, gender equity, and literacy offers a powerful pathway to resilient, broad-based economic growth and financial empowerment (Kajol et al., 2022).

The second most popular theme, *security technologies*, includes subthemes authentication protocols, blockchain, encryption, tokenization, biometrics, multi-factor authentication, risk management, firewall protection, network encryption, and data confidentiality (Chaudhry et al., 2016; Ducas & Wilner, 2017; Huang et al., 2024; Lai et al., 2023; Wang, 2021). Security technologies have become an essential foundation in the digital age, underpinning the confidentiality, integrity, and availability of information systems across sectors. According to extant literature, security technologies encompass a range of mechanisms designed to protect systems from internal and external threats, with increasing emphasis on layered and adaptive strategies (Chawla & Joshi, 2019). One of the sub-themes is authentication protocols. User authentication procedures at the same time are the first layer of defense against intruders. Over time, these protocols have progressed from simple password-based systems to multi-factor authentication (MFA) solutions which combine factors of possession, knowledge and inherence (Cheng et al., 2021). Biometrics systems (fingers, irises or eyelids, faces) use characteristics of physiological variables and have been well documented in leading academic journals for significantly improving access control. However, serious concerns have been raised in regards to violations of privacy and other forms of potential exploitative use as well (Liébaná-Cabanillas et al., 2018). Preserving the privacy of the data over insecure transmission channels, eavesdropping is a critical issue and the implementation of symmetric algorithms such as the advanced security standard specification AES and asymmetric schemes such as the RSA is essential and a proven fact when the efficiency of transmission lines is examined empirically (Roh et al., 2023).

Complementary technology is tokenization, that replaces sensitive data with non-sensitive equivalents (tokens)—especially effective in protecting payment systems and personal identifiable information (PII), as explained in high-ranking publications like Information Systems Frontiers (Tomić et al., 2023). In addition, blockchain technology is receiving substantial attention from scholars for its decentralized, tamper-resistant structure that ensures transaction traceability and transparency without needing areas of centralized trust. Specifically, its cryptographic underpinnings and distributed consensus mechanisms are researched for applications in secure digital identity management, smart contracts, and financial systems resilience (De Reuver et al., 2015). At the same time, firewall security and public network intrusion detection systems (NIDS) are key pieces of perimeter protection, filtering inbound and outbound traffic to detect and stop malicious activity. These technologies are increasingly using different forms of artificial intelligence to make threat detection more accurate and flexible (Ma et al., 2023). According to the literature, a comprehensive synthesis of these sub-components is a necessity in a data - and connectivity - rich environment for mitigating against existing hazards and preparing for potential dangers.

As the third most evident topic, the cashless economy is classified under the core theme, encompassing digital transactions, mobile payments, online banking, payment gateways, cryptocurrency integration, e-wallet adoption, financial inclusion, contactless payments, cyber security, real-time transfers, payment infrastructure, and fintech innovations (Abbasi et al., 2022; Azman Ong et al., 2023; Bednarz et al., 2024; Hossain et al., 2020; Hung et al., 2024; Jin & Liu, 2024). A cashless economy denotes an economic arrangement in which monetary exchanges are settled through digital instruments rather than notes and coins. The transition towards cashless economies is driven by rapid fintech innovations, policy support, and digital infrastructure expansion. The currency used for these systems is digital, supporting fast and transparent transactions that lower costs and enhance traceability. Mass extension of mobile payments and e-wallets such as Paytm, Google Pay, M-Pesa indicates that people are becoming increasingly comfortable about using simple, secure and quick alternative platforms (Berg & Kim, 2022). The online banking sector has also been gaining ground, with 24-hour account management and digital banking services which have replaced conventional banking requirements. Underpinning these advancements are reliable payment gateways and payment systems that facilitate the seamless interactivity among banks, consumers and businesses (Yao et al., 2022). Furthermore, with real-time fund transfers (via, for instance, India's UPI or Europe's SEPA Instant) settlement times have reduced significantly. Cryptocurrency integration, although in its infancy, is emerging as a decentralized alternative, offering transparency and lower remittance costs but raising concerns about regulation and cybersecurity

(Alghamdi et al., 2024). The cashless shift promotes financial inclusion, particularly in remote and underserved areas, by lowering entry barriers through digital onboarding and contactless payments, especially after COVID-19. However, scholars emphasize the need to strengthen digital literacy and cybersecurity frameworks to mitigate fraud and data breaches. Overall, the cashless economy represents a convergence of technology, finance, and policy, reshaping how value is exchanged in modern societies and paving the way for inclusive, efficient financial ecosystems (Huang et al., 2024).

Moving on to the fourth theme which belongs to the motor theme “*digital literacy*” which includes sub-themes such as financial awareness, cyber hygiene, user authentication, digital onboarding, mobile wallets, payment interfaces, consumer protection, fraud detection, data privacy, bank integration, usage behavior, and interface accessibility (Pal et al., 2021; Prasetyo et al., 2025; van Zeeland & Pierson, 2024; Vanini et al., 2023; Wei et al., 2024). Digital literacy, as conceptualized in extant literature, refers to an individual's ability to access, understand, evaluate, and effectively use digital technologies, especially within financial ecosystems. A solid level of financial knowledge combined with an advanced skill level working beyond mere compliance-based operational expertise is essential to facilitate well-behaved monetary decisions in today's digital environment. Empirical findings indicate that digital literacy empowers individuals to effectively complete the requirements of digital banking onboarding (for instance, e-KYC), thereby paving the way for their successful integration into established financial ecosystems. Furthermore, digital literacy equips users with the critical competencies required to safely manage mobile wallets and payments through platforms such as UPI and IMPS; it falls to users to understand the operational rules, transactions norms, and associated cost models of these mechanisms (Pal et al., 2021). Previous research has highlighted that cyber hygiene - everyday practices being taken to secure the online space, such as identifying fake email complaints, using complex passwords, and managing devices to balance the advantages between trust and risk - has been identified as the foundation for digital literacy (Akanfe et al., 2023). The literature stresses that digital literacy also involves fraud and consumer protection aspects, and gives consumers the capability to recognise potential fraudulent activity and to report incidences of fraud and scams (Azman Ong et al., 2023). Next, interface accessibility, including language recognition and interface design, disability inclusion and sensitivity is considered as a critical aspect of digital finance democratization (Akanfe et al., 2023). As such, digital literacy is a complex concept at the core of which is empowering and safe financial inclusion in the digital market.

“*Fraud detection*” which belongs to the niche theme is the rising concern in this digital revolution 5.0. This includes sub-themes such as two-factor authentication, tokenization methods, geolocation tracking, device fingerprinting, transaction monitoring, algorithmic detection, rule-based systems, ai models, anomaly detection, behavior analytics, and real-time monitoring (Antoniou & Batten, 2011; Ayo & Ukpere, 2010; Jin & Liu, 2024; Ramanathan et al., 2022; Shaw et al., 2022). Fraud detection has emerged as a critical component of financial systems, cybersecurity, and e-commerce, necessitating a multidimensional approach that integrates both rule-based and algorithmic mechanisms. Fraud detection is increasingly reliant on real-time monitoring systems that combine static rules with dynamic data analytics to identify suspicious activities. Two-factor authentication (2FA) is widely adopted to enhance identity verification by requiring users to provide two distinct forms of credentials, thereby minimizing unauthorized access (Bommer et al., 2022). Tokenization methods which replace sensitive data with non-sensitive equivalents—play a crucial role in protecting personal and payment information during digital transactions (Cheng et al., 2021). Advanced geolocation tracking aids in validating transactions based on user location patterns, while device fingerprinting collects browser and hardware attributes to uniquely identify devices, thereby detecting anomalies in access points (Al-Okaily et al., 2020). Transaction monitoring systems, supported by algorithmic detection methods, scrutinize behavioral patterns, spending history, and contextual variables in real time. While rule-based systems offer transparency and quick deployment, they are often complemented by AI models, particularly deep learning and ensemble methods, which adaptively learn from vast data inputs to uncover complex fraud schemes (Johnson et al., 2018). Anomaly leverages statistical and machine learning methods to flag deviations from normal behavior, and behavioral analytics refines these insights by profiling user habits. The integration of these techniques ensures a robust, responsive fraud detection ecosystem.

The next niche theme is “*payment evolution*” which includes sub-themes such as digital wallets, fintech innovations, mobile wallets, UPI, NFC payments, cryptocurrency, contactless systems, and virtual banking (de Blanes Sebastián et al., 2023; Hoque et al., 2024; Ramos-de-Luna et al., 2016; Tang et al., 2021; van Zeeland & Pierson, 2024; Zhao et al., 2019). The global transition from traditional cash and card-based payments to digital means of payment is a paradigm shift. Platforms like PayPal and Apple Pay offer digital wallets, which combine bank accounts with consumer-facing tools (such as mobile phones, tablets) for secure transactions in real time. Decentralized financial services enabled by Fintech innovations, especially in developing countries (Dijmarescu et al., 2022). Consequently, transaction fees are lower and individuals who have hitherto been ignored by big banks can now participate in the financial system as well. Mobile wallets like M-Pesa have been able to gain rapid popularity in a short time mainly because as smartphone penetration grows, access to financial tools is always available on the go by cellphone (Abbasi et al., 2022). In India, the introduction of Unified Payments Interface (UPI) has transformed peer-to-peer and merchant

transactions, making it possible for even the tiniest transfer to be settled in real time through biometric authentication supported on a bank's real-time API (Pal et al., 2021). Similarly, contactless payments based on proximity technologies like Near Field Communication (NFC)-devices linked to cell phones, etc. have been gaining popularity post-COVID-19. Cryptocurrencies such as Bitcoin and Ethereum are decentralized and borderless methods of payment. However, regulatory uncertainty and high volatility limit their widespread use as yet (Liu et al., 2025). Further, wearables and QR code scans with contactless payments have streamlined low-value transactions, increasing their speed and hygiene. Finally, neobanks or virtual financial institutions are entirely operational and don't rely on physical branches to deliver service. Relying instead on artificial intelligence and big data processing they reshape traditional banking models in unfamiliar ways. Together, these trends in payment illustrate a return to more efficient and better user-centred methods of finance (Bednarz et al., 2024).

Moving towards our final theme, i.e., number seventh, i.e., “*regulatory compliance*,” which includes sub-themes such as data privacy, transaction monitoring, KYC regulations, AML compliance, licensing requirements, cybersecurity framework, encryption standards, third-party oversight, payment authentication, regulatory technology, and real-time surveillance (Agarwal et al., 2024; Azman Ong et al., 2023; Berg & Kim, 2022; Ducas & Wilner, 2017; Liu et al., 2024). Financial institutions are obligated to comply with data protection regimes such as the GDPR and India's DPDP Act, safeguarding customer data from unauthorized access. Furthermore, regulatory technology (RegTech) and real-time surveillance systems, are enabling proactive compliance through automated monitoring and reporting. Together, these sub-themes form a comprehensive compliance architecture that aligns digital finance with evolving regulatory expectations.

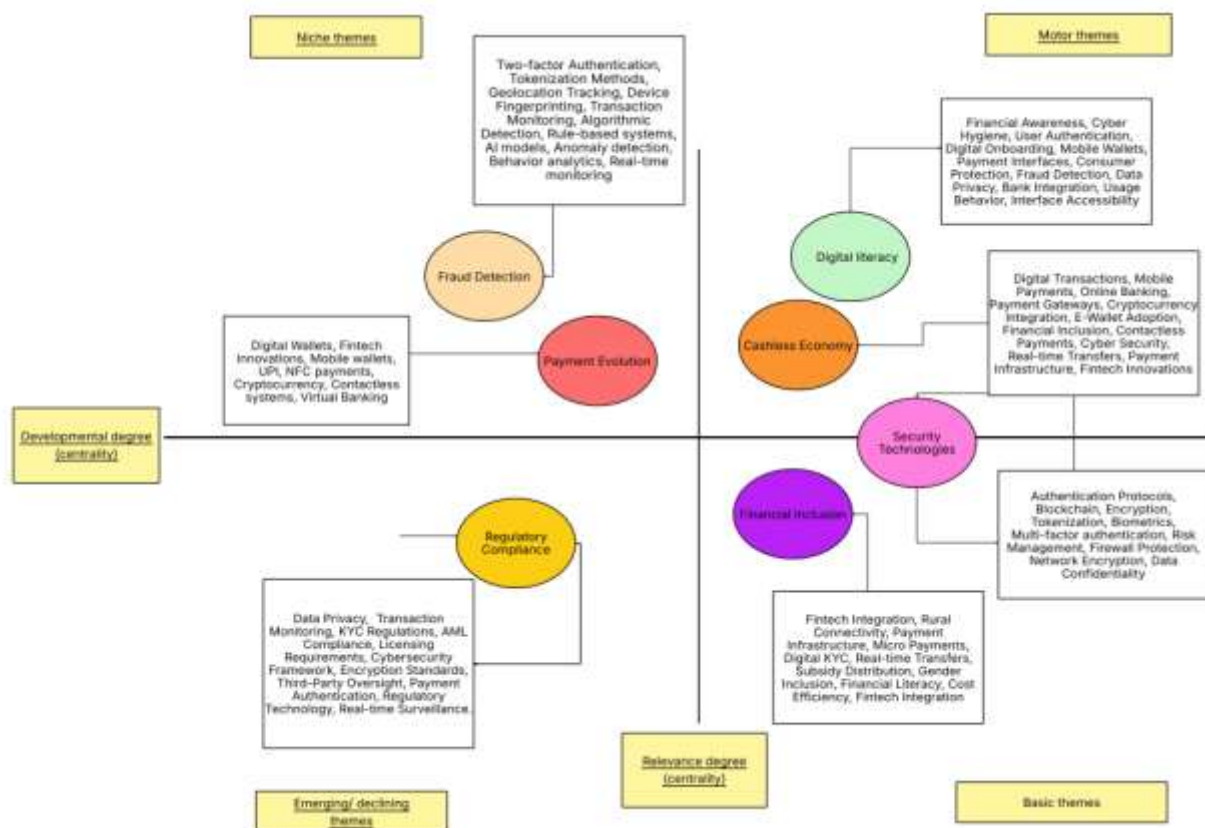


Figure 2 Thematic Map

3.2. Conceptual framework

A conceptual framework is an organized schematic—visual or textual—that delineates the principal variables and constructs of an inquiry and articulates their posited interrelationships. Grounded in extant theory and systematic interpretation of the literature, it serves as the architectural backbone of the study (Bansal et al., 2025). Moreover, a well-defined framework enhances the internal coherence and consistency of a research paper. It aligns the literature review, methodology, data analysis, and discussion with the study's theoretical foundations. Conceptual frameworks

improve the validity and rigor of research by providing a logical flow and rationale for variable selection, sampling, and analytical strategies.

With the era of dynamic technologies and rising digital payments, there has been a huge need for smart technologies and regulatory compliance. Therefore, our study has developed a conceptual framework defining framework to achieve regulatory compliance, which overall impacts SDG 9, i.e., industry innovation and infrastructure. Security technologies including encryption standards, biometric authentication, two-factor authentication, and end-to-end transaction security play a foundational role in fostering user trust in digital platforms (van Zeeland & Pierson, 2024). When individuals perceive digital environments as secure, they are more likely to engage, explore, and interact with digital tools, thereby enhancing their digital literacy. Digital literacy, as defined in literature, refers not only to the technical ability to use digital devices but also to critical thinking, information management, and financial behavior within digital ecosystems (Xia et al., 2023). As users become more digitally literate, they develop the confidence and competence to shift away from physical cash transactions, accelerating the movement towards a cashless economy, wherein digital payments replace traditional forms of currency (Vanini et al., 2023). This transition fuels payment evolution, characterized by increased adoption of mobile wallets, UPI, contactless cards, and QR-based payments, which are more efficient and traceable. In turn, these digital payment infrastructures serve as enablers for financial inclusion, particularly for underbanked populations in rural and semi-urban regions, by reducing geographic, economic, and literacy-related barriers. As empirical evidence, this sequential linkage from security-driven digital literacy to economic inclusion creates a self-reinforcing ecosystem where technological trust and user capability drive broader access to and usage of formal financial services (Hung et al., 2024).

As with increasing use of mobile wallets, real-time transfers and interoperable platforms, all transactions generate a digital trail that can be followed. This abundance of structured data creates the optimal conditions to implement advanced fraud-detection algorithms, including anomaly-detection algorithms driven by artificial intelligence, machine-learning models, and real-time monitoring tools that are currently considered the pinnacle of tools within modern financial services (Wei et al., 2024). In addition, more financial inclusion, especially when based on digital identities and e-KYC norms, means that users are formally brought into the financial system. This makes it possible to enhance customer verification levels and give credit worthiness profiles to every user. Which means a more transparent and audit-friendly environment, and higher standards of regulatory compliance for areas where the laws demand it, such as AML (Anti-Money Laundering), KYC and real-time transaction monitoring (Agarwal et al., 2024). The literature emphasizes that when fraud detection is embedded in the financial infrastructure, it can support dynamic policy enforcement and maintain adherence to international standards of regulation; and this is especially relevant for emerging markets (Dimitrova & Öhman, 2024). Collectively, these outcomes enhance financial integrity, reduce systemic risk, and support the development of resilient infrastructure and inclusive innovation, as envisioned under SDG 9 (Hoque et al., 2024). Thus, the chain from digital enablement to cashless systems ultimately cultivates a trusted, compliant, and innovation-driven financial ecosystem critical for sustainable economic growth.



Figure 3 Conceptual Framework

4. FUTURE RESEARCH DIRECTIONS

The Future Research Agenda in a research report delineates the suggested trajectories for future investigations, informed by the results, limits, and developing enquiries of the current study. It functions as a resource for researchers aiming to expand upon current scholarship by pinpointing deficiencies in the literature, suggesting novel theoretical frameworks, or examining the subject across other contexts or demographics. This goal frequently emphasises aspects that were either outside the purview of the current study or require further examination, promoting methodological innovation and multidisciplinary strategies.

Table 1 Future research directions

Quadrant	Theme	Future Research Questions
Basic Theme	Financial Inclusion	To what extent can the integration of digital financial technologies (such as mobile banking, UPI, and digital wallets) bridge the financial access gap in remote and marginalized regions, especially where traditional banking infrastructure is absent?
		How do socio-cultural factors, digital literacy levels, and regulatory policies influence the adoption and impact of financial inclusion initiatives among underbanked populations, particularly women and rural citizens?
		How can real-time digital payment systems and low-cost infrastructure be optimized to sustainably scale financial inclusion while maintaining data privacy, affordability, and security?
Basic Theme	Security Technologies	How can advanced security frameworks incorporating multi-factor authentication, blockchain, and biometric systems be designed to ensure end-to-end protection of user data across digital financial platforms?
		In what ways can artificial intelligence and machine learning-based predictive models be used to proactively mitigate cybersecurity threats and financial fraud in real-time financial transactions?
		What are the key trade-offs between user convenience and data protection in implementing security protocols, and how can these be balanced in the context of growing digital payment adoption?
Motor Theme	Cashless Economy	What are the long-term behavioral, technological, and infrastructural determinants of consumer transition from cash-based transactions to digital payment modes across different socio-economic groups?
		How does the shift towards a cashless economy influence macroeconomic stability, informal sector inclusion, and financial transparency in emerging economies like India?
		What role should governments and regulatory authorities play in incentivizing digital payment adoption and addressing infrastructural gaps in order to build a resilient, inclusive cashless economy?
Motor Theme	Digital Literacy	How does digital literacy, encompassing knowledge of cybersecurity, mobile banking interfaces, and digital onboarding processes, influence the uptake and safe usage of fintech platforms across age, gender, and regional demographics?
		How can public-private partnerships, fintech firms, and educational institutions collaborate to design scalable, inclusive, and culturally sensitive digital literacy programs tailored to the needs of the financially excluded?
		What is the empirical relationship between digital literacy and reduction in financial fraud, improved user confidence, and increased participation in digital finance ecosystems?

Niche Theme	Fraud Detection	How can next-generation fraud detection systems, using technologies like AI-driven anomaly detection, biometric verification, and geolocation tracking, be tailored to detect complex, real-time financial crimes in a decentralized environment?
		What are the legal, ethical, and data privacy implications of using behavioral analytics and predictive algorithms for fraud detection in fintech, and how can these concerns be addressed through policy and design?
		How can machine learning models be continuously updated and trained on diverse datasets to minimize false positives and adapt to evolving fraud tactics in the global digital economy?
Niche Theme	Payment Evolution	How has the rapid evolution of payment technologies—from physical cash to contactless payments, mobile wallets, and cryptocurrency—transformed consumer behavior, merchant engagement, and transaction efficiency?
		What are the infrastructural, regulatory, and technological enablers and barriers to the widespread adoption of interoperable digital payment ecosystems in developing nations?
		How do socio-economic factors and digital readiness influence the acceptance, resistance, or delayed adoption of newer payment innovations across different geographies?
Emerging Theme	Regulatory Compliance	What is the effectiveness of current digital regulatory instruments (e.g., transaction monitoring, licensing, encryption standards) in preventing fraud, ensuring privacy, and fostering trust in digital financial services?
		How do differences in global regulatory regimes impact cross-border digital financial transactions, and what models of regulatory harmonization or sandboxing could be adopted to address these challenges?
		What role can RegTech solutions play in automating real-time surveillance, anti-money laundering (AML) procedures, and cross-border KYC validations while ensuring data sovereignty and user consent?

CONCLUSION

The success of EPS has changed access, speed, and simplicity of money transactions and even the nature of economic transactions. As nations move towards becoming cashless societies, e-payment systems have played a vital role in driving financial inclusion and digital migration forward. Yet this development is accompanied by an ever more sophisticated and technical landscape of security vulnerabilities and financial manipulative methods that counterfeit the legitimacy of user and system interactions. This paper explained technical, behavioural and regulatory aspects for EPS security and stressed the need for a comprehensive and multi-layered approach to fraud prevention. The report points to the fact that while cutting edge technologies such as biometrics, artificial intelligence, tokenization and encryption are the foundations of digital security, these are effective only when coupled with proper regulatory adherence to best practices and greater digital literacy by users. The conceptual framework developed in this paper places regulatory compliance at the core, supported by secure technologies, informed users, and inclusive financial

practices. This interconnected framework directly contributes to the achievement of SDG-9 (Industry, Innovation, and Infrastructure) by fostering resilient digital financial ecosystems.

Going forward, policymakers, fintech innovators, educators, and financial institutions must collaborate to ensure that EPS not only remain technologically secure but also socially equitable and development oriented. A secure, inclusive, and intelligently regulated EPS landscape is not just a technological necessity it is a fundamental enabler of sustainable economic growth.

REFERENCES

- Abbasi, G. A., Sandran, T., Ganesan, Y., & Iranmanesh, M. (2022). Go cashless! Determinants of continuance intention to use E-wallet apps: A hybrid approach using PLS-SEM and fsQCA. *Technology in Society*, 68. <https://doi.org/10.1016/j.techsoc.2022.101937>
- Agarwal, S., Ghosh, P., Ruan, T., & Zhang, Y. (2024). Transient Customer Response to Data Breaches of Their Information. *Management Science*, 70(6), 4105–4114. <https://doi.org/10.1287/mnsc.2021.01335>
- Akanfe, O., Valecha, R., & Rao, H. R. (2023). Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services. *IEEE Transactions on Engineering Management*, 70(3), 864–876. <https://doi.org/10.1109/TEM.2020.3015222>
- Al-Okaily, M., Lutfi, A., Alsaad, A., Taamneh, A., & Alsyouf, A. (2020). The Determinants of Digital Payment Systems' Acceptance under Cultural Orientation Differences: The Case of Uncertainty Avoidance. *Technology in Society*, 63. <https://doi.org/10.1016/j.techsoc.2020.101367>
- Alghamdi, S., Daim, T., & Alzahrani, S. (2024). Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment. *IEEE Transactions on Engineering Management*, 71, 7701–7718. <https://doi.org/10.1109/TEM.2024.3376314>
- Antoniou, G., & Batten, L. (2011). E-commerce: Protecting purchaser privacy to enforce trust. *Electronic Commerce Research*, 11(4), 421–456. <https://doi.org/10.1007/s10660-011-9083-3>
- Aparicio, G., Iturralde, T., & Maseda, A. (2019). Conceptual structure and perspectives on entrepreneurship education research: A bibliometric review. *European Research on Management and Business Economics*, 25(3), 105–113. <https://doi.org/10.1016/j.iedeen.2019.04.003>
- Ayo, C. K., & Ukpere, W. I. (2010). Design of a secure unified e-payment system in Nigeria : A case study. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, 4(9), 1753–1760. <http://www.academicjournals.org/AJBM>
- Azman Ong, M. H., Yusri, M. Y., & Ibrahim, N. S. (2023). Use and behavioural intention using digital payment systems among rural residents: Extending the UTAUT-2 model. *Technology in Society*, 74. <https://doi.org/10.1016/j.techsoc.2023.102305>
- Bajwa, F. A., Fu, J., Bajwa, I. A., Ahmad, S., & Mahmood, F. (2025). Factors influencing usage and loyalty for payment app customers in Saudi Arabia. *Acta Psychologica*, 255. <https://doi.org/10.1016/j.actpsy.2025.104961>
- Bansal, S., Kumar, S., Ali, S., Singh, S., Nangia, P., & Bamel, U. (2024). Harnessing Digital Finance for Sustainability: An Integrative Review and Research Agenda. *Research in International Business and Finance*, 102682. <https://doi.org/10.1016/j.ribaf.2024.102682>
- Bansal, S., Nangia, P., & Koles, B. (2025). Neuromarketing and the Marketing Mix: An Integrative Review and Future Research Agenda Using the TMC Approach. *International Journal of Consumer Studies*, 49(3). <https://doi.org/10.1111/ijcs.70072>
- Bednarz, J., Markiewicz, M., & Szmelter-Jarosz, A. (2024). Digital payments during the COVID-19 pandemic in Poland: An initial insight on the consumer perception of security and convenience. *Argumenta Oeconomica*, 52(1), 115–144. <https://doi.org/10.15611/aoe.2024.1.07>
- Berg, N., & Kim, J. Y. (2022). Optimal online-payment security system and the role of liability sharing. *Economic Modelling*, 110. <https://doi.org/10.1016/j.econmod.2022.105805>
- Bommer, W. H., Rana, S., & Milevoj, E. (2022). A meta-analysis of eWallet adoption using the UTAUT model. *International Journal of Bank Marketing*, 40(4), 791–819. <https://doi.org/10.1108/IJBM-06-2021-0258>
- Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2016). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. *Electronic Commerce Research*, 16(1), 113–139. <https://doi.org/10.1007/s10660-015-9192-5>
- Chawla, D., & Joshi, H. (2019). Consumer attitude and intention to adopt mobile wallet in India – An empirical study. *International Journal of Bank Marketing*, 37(7), 1590–1618. <https://doi.org/10.1108/IJBM-09-2018-0256>
- Cheng, X., Hou, T., & Mou, J. (2021). Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. *Information and Management*, 58(6). <https://doi.org/10.1016/j.im.2021.103450>
- Cobo, M. J., Martínez, M. A., Gutiérrez-Salcedo, M., Fujita, H., & Herrera-Viedma, E. (2015). 25years at Knowledge-Based Systems: A bibliometric analysis. *Knowledge-Based Systems*, 80, 3–13.

<https://doi.org/10.1016/j.knosys.2014.12.035>

- Cotugno, M., Manta, F., Perdichizzi, S., & Stefanelli, V. (2024). Ready for a digital Euro? Insights from a research agenda. *Research in International Business and Finance*, 67. <https://doi.org/10.1016/j.ribaf.2023.102117>
- De Blanes Sebastián, M. G., Antonovica, A., & Sarmiento Guede, J. R. (2023). What are the leading factors for using Spanish peer-to-peer mobile payment platform Bizum? The applied analysis of the UTAUT2 model. *Technological Forecasting and Social Change*, 187. <https://doi.org/10.1016/j.techfore.2022.122235>
- De Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N., & Bouwman, H. (2015). Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators. *Electronic Commerce Research and Applications*, 14(5), 331–344. <https://doi.org/10.1016/j.elerap.2014.08.004>
- Dijmarescu, I., Iatagan, M., Hurloiu, I., Geamanu, M., Rusescu, C., & Dijmarescu, A. (2022). Neuromanagement decision making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. *Oeconomia Copernicana*, 13(1), 225–250. <https://doi.org/10.24136/oc.2022.007>
- Dimitrova, I., & Öhman, P. (2024). Flip that coin: Barriers, barrier-breakers, and full-adoption of digital payment methods. *Journal of Consumer Behaviour*, 23(5), 2367–2378. <https://doi.org/10.1002/cb.2343>
- Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal*, 72(4), 538–562. <https://doi.org/10.1177/0020702017741909>
- El Hloul, F. Z., Riffi, J., Sayyouri, M., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2023). Detecting Fraudulent Transactions Using Stacked Autoencoder Kernel ELM Optimized by the Dandelion Algorithm. *Journal of Theoretical and Applied Electronic Commerce Research*, 18(4), 2057–2076. <https://doi.org/10.3390/jtaer18040103>
- Fagerberg, J., Fosaas, M., & Sapprasert, K. (2018). Innovation: Exploring the knowledge base. *Innovation, Economic Development and Policy: Selected Essays*, 41(7), 160–181. <https://doi.org/10.1016/j.respol.2012.03.008>
- Hart, C. (1998). The literature review in research: Releasing the social science imagination. In *Doing a Literature Review* (p. pp.01-25). https://books.google.co.zw/books?id=FkXvY8oDFdsC&printsec=frontcover&source=gbs_ge_summary
- Hoque, M. E., Susanto, P., Shah, N. U., Khatimah, H., & Mamun, A. Al. (2024). Does perceived behavioral control mediate customers' innovativeness and continuance intention of e-money? The moderating role of perceived risk and e-security. *International Journal of Emerging Markets*, 19(12), 4481–4502. <https://doi.org/10.1108/IJOEM-06-2022-0914>
- Hossain, S. F. A., Xi, Z., Nurunnabi, M., & Hussain, K. (2020). Ubiquitous Role of Social Networking in Driving M-Commerce: Evaluating the Use of Mobile Phones for Online Shopping and Payment in the Context of Trust. *SAGE Open*, 10(3). <https://doi.org/10.1177/2158244020939536>
- Huang, S. Y., Wang, T., Huang, Y. T., & Yeh, T. N. (2024). Information security risk items and management practices for mobile payment using non-financial-institution service providers: An exploratory study. *International Journal of Accounting Information Systems*, 53. <https://doi.org/10.1016/j.accinf.2024.100684>
- Hung, S. W., Cheng, M. J., & Tung, Y. J. (2024). Following the herd? An empirical investigation into the adoption of mobile payment systems. *International Journal of Bank Marketing*, 42(5), 897–923. <https://doi.org/10.1108/IJBM-03-2023-0195>
- Jin, L., & Liu, M. (2024). Unlocking Financial Opportunities: The Substantial Alleviation of Financing Constraints on Small and Micro Enterprises Through Digital Inclusive Finance. *Journal of the Knowledge Economy*. <https://doi.org/10.1007/s13132-024-01863-7>
- Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior*, 79, 111–122. <https://doi.org/10.1016/j.chb.2017.10.035>
- Kable, A. K., Pich, J., & Maslin-Prothero, S. E. (2012). A structured approach to documenting a search strategy for publication: A 12 step guideline for authors. *Nurse Education Today*, 32(8), 878–886. <https://doi.org/10.1016/j.nedt.2012.02.022>
- Kajol, K., Singh, R., & Paul, J. (2022). Adoption of digital financial transactions: A review of literature and future research agenda. *Technological Forecasting and Social Change*, 184. <https://doi.org/10.1016/j.techfore.2022.121991>
- Lai, K. K., Chen, Y. L., Kumar, V., Daim, T., Verma, P., Kao, F. C., & Liu, R. (2023). Mapping technological trajectories and exploring knowledge sources: A case study of E-payment technologies. *Technological Forecasting and Social Change*, 186. <https://doi.org/10.1016/j.techfore.2022.122173>
- Laksamana, P., Suharyanto, S., & Cahaya, Y. F. (2023). Determining factors of continuance intention in mobile payment: fintech industry perspective. *Asia Pacific Journal of Marketing and Logistics*, 35(7), 1699–1718. <https://doi.org/10.1108/APJML-11-2021-0851>

- Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higuera-Castillo, E. (2024). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information and Management*, 61(2). <https://doi.org/10.1016/j.im.2023.103907>
- Liébana-Cabanillas, F., Marinkovic, V., Ramos de Luna, I., & Kalinic, Z. (2018). Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach. *Technological Forecasting and Social Change*, 129, 117–130. <https://doi.org/10.1016/j.techfore.2017.12.015>
- Lisana, & Handarkho, Y. D. (2023). Social aspect versus service quality in trust formation toward mobile payment adoption: a case study of Indonesia. *Asia Pacific Journal of Marketing and Logistics*, 35(6), 1349–1365. <https://doi.org/10.1108/APJML-10-2021-0774>
- Liu, X., Wang, Q., Wu, G., & Zhang, C. (2024). Determinants of individuals' intentions to use central bank digital currency: evidence from China. *Technology Analysis and Strategic Management*, 36(9), 2213–2227. <https://doi.org/10.1080/09537325.2022.2131517>
- Liu, X., Wu, J., & Zhang, C. (2025). Antecedents of consumers' acceptance of central bank digital currency: The role of technology perceptions, social influence and personal traits. *Technological Forecasting and Social Change*, 217. <https://doi.org/10.1016/j.techfore.2025.124192>
- Ma, C., Wu, J., Sun, H., Zhou, X., & Sun, X. (2023). Enhancing user experience in digital payments: A hybrid approach using SEM and neural networks. *Finance Research Letters*, 58. <https://doi.org/10.1016/j.frl.2023.104376>
- Mohd Thas Thaker, H., Subramaniam, N. R., Qoyum, A., & Iqbal Hussain, H. (2023). Cashless society, e-wallets and continuous adoption. *International Journal of Finance and Economics*, 28(3), 3349–3369. <https://doi.org/10.1002/ijfe.2596>
- Nangia, P., Bansal, S., & Thaichon, P. (2024). Doing more with less: An integrative literature review on responsible consumption behaviour. *Journal of Consumer Behaviour*, 23(1), 141–155. <https://doi.org/10.1002/cb.2163>
- Oney, E., Guven, G. O., & Rizvi, W. H. (2017). The determinants of electronic payment systems usage from consumers' perspective. *Economic Research-Ekonomika Istrazivanja*, 30(1), 394–415. <https://doi.org/10.1080/1331677X.2017.1305791>
- Pal, A., Herath, T., De', R., & Raghav Rao, H. (2021). Why do people use mobile payment technologies and why would they continue? An examination and implications from India. *Research Policy*, 50(6), 104228. <https://doi.org/10.1016/j.respol.2021.104228>
- Prasetyo, Y. T., Susanto, K. C., Chuang, K. H., Yin, R. T., Chen, J. W., Zhang, Y. X., Benito, O. P., Belmonte, Z. J. A., Cahigas, M. M. L., Nadlifatin, R., & Gumasing, M. J. J. (2025). Factors influencing the perceived usability of line pay: An extended technology acceptance model approach. *Acta Psychologica*, 255. <https://doi.org/10.1016/j.actpsy.2025.104924>
- Rajaguru, R. (2024). Effects of contemporary technologies, such as blockchain and artificial intelligence (AI) in enhancing consumers' trustworthiness of online reviews. *Journal of Hospitality Marketing and Management*, 33(2), 251–259. <https://doi.org/10.1080/19368623.2023.2258522>
- Ramanathan, U., Williams, N. L., Zhang, M., Sa-Nguanjin, P., Garza-Reyes, J. A., & Borges, L. A. (2022). A New Perspective of E-Trust in the Era of Social Media: Insights From Customer Satisfaction Data. *IEEE Transactions on Engineering Management*, 69(4), 1417–1431. <https://doi.org/10.1109/TEM.2020.2985379>
- Ramos-de-Luna, I., Montoro-Ríos, F., & Liébana-Cabanillas, F. (2016). Determinants of the intention to use NFC technology as a payment system: an acceptance model approach. *Information Systems and E-Business Management*, 14(2), 293–314. <https://doi.org/10.1007/s10257-015-0284-5>
- Rodríguez-Soler, R., Uribe-Toril, J., & De Pablo Valenciano, J. (2020). Worldwide trends in the scientific production on rural depopulation, a bibliometric analysis using bibliometrix R-tool. *Land Use Policy*, 97, 104787. <https://doi.org/10.1016/j.landusepol.2020.104787>
- Roh, T., Park, B. Il, & Xiao, S. (2023). Adoption of Ai-Enabled Robo-Advisors in Fintech: Simultaneous Employment of Utaut and the Theory of Reasoned Action. *Journal of Electronic Commerce Research*, 24(1), 29–47. https://www.researchgate.net/profile/Taewoo-Roh/publication/369529899_Adoption_of_AI-enabled_Robo-advisors_in_fintech_Simultaneous_employment_of_UTAUT_and_the_theory_of_reasoned_action/links/641f983d315dfb4cceab0fee/Adoption-of-AI-enabled-Robo-advisors-in-fintech-Simultaneous-employment-of-UTAUT-and-the-theory-of-reasoned-action.pdf
- Seuring, S., & Müller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. *Journal of Cleaner Production*, 16(15), 1699–1710. <https://doi.org/10.1016/j.jclepro.2008.04.020>
- Shaw, N., Eschenbrenner, B., & Brand, B. M. (2022). Towards a Mobile App Diffusion of Innovations model: A multinational study of mobile wallet adoption. *Journal of Retailing and Consumer Services*, 64. <https://doi.org/10.1016/j.jretconser.2021.102768>
- Taneja, S., Ali, L., Siraj, A., Ferrasso, M., Luthra, S., & Kumar, A. (2024). Leveraging Digital Payment

Adoption Experience to Advance the Development of Digital-Only (Neo) Banks: Role of Trust, Risk, Security, and Green Concern. *IEEE Transactions on Engineering Management*, 71, 10862–10873.

<https://doi.org/10.1109/TEM.2024.3395130>

- Tang, Y. M., Chau, K. Y., Hong, L., Ip, Y. K., & Yan, W. (2021). Financial innovation in digital payment with wechat towards electronic business success. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5), 1844–1861. <https://doi.org/10.3390/jtaer16050103>
- Tomić, N., Kalinić, Z., & Todorović, V. (2023). Using the UTAUT model to analyze user intention to accept electronic payment systems in Serbia. *Portuguese Economic Journal*, 22(2), 251–270. <https://doi.org/10.1007/s10258-022-00210-5>
- Van Zeeland, I., & Pierson, J. (2024). Changing the whole game: effects of the COVID-19 pandemic's accelerated digitalization on European bank staff's data protection capabilities. *Financial Innovation*, 10(1). <https://doi.org/10.1186/s40854-023-00533-y>
- Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation*, 9(1). <https://doi.org/10.1186/s40854-023-00470-w>
- Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, 7(1). <https://doi.org/10.1186/s40854-021-00260-2>
- Wei, Y., Gáti, M., & Simay, A. E. (2024). How consumers' privacy perceptions influenced mobile payment acceptance during the COVID-19 pandemic. *International Journal of Bank Marketing*, 42(7), 2051–2074. <https://doi.org/10.1108/IJBM-04-2023-0245>
- Xia, H., Gao, Y., & Zhang, J. Z. (2023). Understanding the adoption context of China's digital currency electronic payment. *Financial Innovation*, 9(1). <https://doi.org/10.1186/s40854-023-00467-5>
- Yao, B. H., Shanoyan, A., Schwab, B., & Amanor-Boadu, V. (2022). Mobile money, transaction costs, and market participation: evidence from Côte d'Ivoire and Tanzania. *Food Policy*, 112. <https://doi.org/10.1016/j.foodpol.2022.102370>
- Zaffar, M. A., Kumar, R., & Zhao, K. (2024). Competitive dynamics in a multi-sided mobile payment platform market: an agent-based modeling perspective. *International Journal of Bank Marketing*, 42(7), 2023–2050. <https://doi.org/10.1108/IJBM-11-2023-0610>
- Zhao, H., Anong, S. T., & Zhang, L. (2019). Understanding the impact of financial incentives on NFC mobile payment adoption: An experimental analysis. *International Journal of Bank Marketing*, 37(5), 1296–1312. <https://doi.org/10.1108/IJBM-08-2018-0229>