

OPEN ACCESS

Volume: 5

Issue: 3

Month: July

Year: 2026

ISSN: 2583-7117

Published: 17.07.2026

Citation:

Suhaib Ahmed Quraishy, Abdulla "Digital Payment Systems: Their Role in Economic Growth and Associated Criminal Activities" International Journal of Innovations in Science Engineering and Management, vol. 5, no. 3, 2026, pp. 113-119

DOI:

10.69968/ijisem.2026v5i3113-119



This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Digital Payment Systems: Their Role in Economic Growth and Associated Criminal Activities

Suhaib Ahmed Quraishy¹, Abdulla²

¹Ph.D. Research scholar, Department of commerce, Mohammad Ali Jauhar University, Rampur, Uttar pradesh, India

²Ph.D. Research scholar, Faculty of Law, Mohammad Ali Jauhar University, Rampur, Uttar pradesh, India

Abstract

Digital payment systems have revolutionized the financial sector, offering secure, efficient, and real-time electronic transactions worldwide. The financial inclusion has been enhanced, business efficiency, e-commerce, and economic growth have been supported with the fast growth of technology like Unified Payments Interface (UPI), mobile wallets, Internet banking, credit and debit cards and QR code based payments. At the same time, the growing reliance on digital financial services has opened up new avenues for financial crimes via cyber means such as phishing, identity theft, QR-code fraud, OTP fraud, money laundering, malware attacks and account takeover. This review aims to analyse the impact of digital payment on economic development and provide an insight into the new security issues surrounding the use of these digital payments. It also examines the contribution that the regulatory framework, security measures, fraud protection systems, consumer understanding and awareness, and institutional cooperation can play in enhancing the security of payments. In conclusion, the review suggests that sustainable digital payment systems need to combine technological innovation, effective regulation, and cybersecurity awareness.

Keywords; Digital Payment Systems; Unified Payments Interface (UPI); Financial Inclusion; Economic Growth; Digital Payment Fraud.

INTRODUCTION

Digital payment systems are redefining the payment landscape, moving financial transactions from a cash-centric economy to a digitally integrated and cashless environment. In the modern era, with the use of information and communication technologies, the general availability of the Internet, the penetration of smartphones and enabling governmental programs, the use of electronic methods of payment has increased in most countries around the world. Today, digital payments involve different tools such as internet banking, debit cards, credit cards, mobile wallet, QR code payments, and real-time payment platforms which are more convenient, rapid, and transparent than traditional cash payments. [1], [2]

Financial technology (fintech) has also transformed digital payment infrastructure, bringing in new and customer-centric payment methods at an unprecedented pace. The Unified Payments Interface (UPI) launched by the National Payments Corporation of India (NPCI) in 2016 was a big break-through for digital financial services in India. With UPI, instant bank-to-bank transfers have been introduced via mobile apps, UPI has been connected with mobile wallets, QR merchant payments and internet banking. The constant growth of fintech platforms and digital payment applications has improved financial inclusion, especially for small enterprises, rural communities, and communities that were previously under-served, thereby solidifying the nation's digital economy. [3], [4]

Digital payment systems play a critical role in modern economic growth and development, contributing to the development of e-commerce, the formalization of

economic activities, the enhancement of business efficiency, and financial inclusion. With the rise of digital transactions has come new opportunities for payment fraud, identity theft, phishing, and money laundering, among others, via cyber means. For this reason, it is important for policymakers, financial institutions and researchers to understand the impact of digital payment systems on the economy as well as the crime risks that are linked to them. [5]

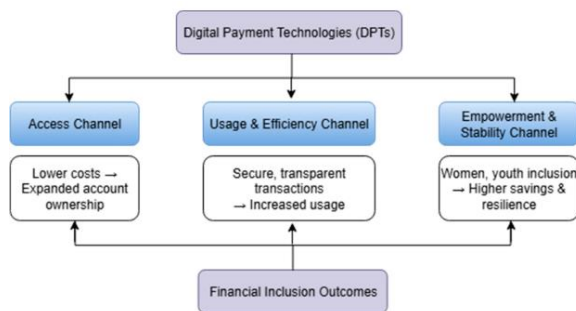


Figure 1: Conceptual framework linking digital payment technologies to financial inclusion outcomes [6].

Digital Payment Systems and Their Contribution to Economic Growth

Digital payment systems have emerged as an integral part of the modern economy, facilitating secure, efficient, and instantaneous financial transactions. They enable the transfer of money from one person to another, from businesses to businesses, and from businesses to governments, without the need for physical cash, and help create a more open financial system. These systems have enabled the rapid growth of economic activities, improved financial infrastructure, and enhanced sustainable economic development [7].

There are various popular digital payment systems available including Unified Payments Interface (UPI), debit and credit cards, mobile wallets, internet banking and QR code-based payment platforms. These payment methods bring convenience, costs are reduced, and funds are transferred instantly, thus making financial services more accessible to various user groups. They have helped to increase the availability of financial services to those who had been excluded or underserved, especially in remote and rural regions, by integrating with fintech innovations [8]. Greater financial inclusion has led to improved savings, access to credit and digital financial literacy and underpinned inclusion in economic development. Moreover, digital payments also make business operations more

efficient by providing faster settlements, cutting down on the operational expenses, and promoting the expansion of Micro, Small, and Medium Enterprise (MSMEs) and e-commerce [9]. They also contribute to greater transparency in taxes by providing a record of transactions that can be traced, smaller informal economy, and better government revenue collection. This brings consumers more convenience and security, businesses more productivity and market access, and governments more efficient public service delivery and transparent public finance management [10].

Table 1: Contribution of Major Digital Payment Systems to Economic Growth

Digital Payment System	Description	Contribution to Economic Growth	Examples
Unified Payments Interface (UPI)	Real-time bank-to-bank payment system enabling instant fund transfers through mobile applications.	Promotes cashless transactions, enhances financial inclusion, supports MSMEs, increases transaction efficiency, and boosts digital commerce.	BHIM UPI, Google Pay, PhonePe, Paytm
Debit and Credit Cards	Electronic payment cards used for online and point-of-sale (POS) transactions.	Increases consumer spending, improves payment convenience, reduces cash handling costs, and strengthens formal financial activities.	Visa, Mastercard, RuPay
Mobile Wallets	Digital applications that store payment information and facilitate electronic transactions.	Encourages digital adoption, improves accessibility for small-value transactions, and supports retail and e-commerce growth.	Paytm Wallet, Amazon Pay, MobiKwik
Internet Banking	Online banking platform that enables fund transfers, bill payments, and	Improves banking accessibility, reduces operational costs, enhances business	Net Banking Services of Commercial Banks

	account management.	efficiency, and supports digital financial services.	
QR Code-Based Payments	Contactless payment method using Quick Response (QR) codes scanned through smartphones.	Simplifies merchant payments, increases digital acceptance among small businesses, lowers transaction costs, and promotes financial inclusion.	Bharat QR, UPI QR

Criminal Activities Associated with Digital Payment Systems

Digital payment systems have enhanced the efficiency and accessibility of financial transactions, but they've also created more opportunities for cyber-based financial crimes. As more and more people rely on technology to pay for goods and services, whether online or with their cell phone or digital banking app, new and expanded opportunities exist for cybercriminals to exploit both technology and human behavior. With the growth of digital transactions, financial institutions, businesses, and consumers are facing more advanced forms of fraud that pose a risk to the security, reliability, and trust of digital payment systems [11].

Overview of Digital Financial Crimes

Digital financial crimes involve illegal activities that use electronic payment systems, online banking platforms, mobile applications and digital financial services to achieve an illegal financial gain. These crimes are also largely cyber-enabled and frequently anonymous, cross-border and technologically sophisticated, in contrast to traditional financial crimes. The growing digitalization of fintech services has paved the way for organized cybercriminals to make digital payment systems easy targets.

Common Forms of Digital Payment Fraud

Digital payment fraud includes all the types of cybercrime such as phishing, QR code fraud, identity theft, one-time password fraud, SIM swapping, fake payment screenshot scams, malware attack, payment card fraud, account takeover, social engineering, and money laundering via digital payment channels. A large proportion of these offences target users' insufficient cyber security awareness, not the vulnerabilities of payment technologies. Banks, payment service providers, and government agencies are often the disguise used by criminals to trick people into

providing their confidential financial information in order to gain access to their bank accounts and make fraudulent withdrawals [12].

Drivers and Economic Implications

The rise in cyber-enabled financial crimes is attributed to the digitalisation, penetration of fintech, and the higher smartphone penetration, lack of cyber-security awareness, and sophistication of cybercriminal networks. These crimes inflict monetary damages, interfere with business operations, diminish consumer trust in electronic transactions, and drive up costs for financial institutions related to compliance and cybersecurity. On the social level, the persistent digital payment fraud negatively impacts trust in digital financial services, financial inclusion programs and can also present challenges to sustainable economic growth. Therefore, bolstering cybersecurity systems, regulatory oversight, and public understanding is crucial for ensuring the long-term sustainability of digital payment systems.

Regulatory Framework and Preventive Measures

Rapidly expanding electronic payment systems have made it essential to have strong regulatory frameworks and extensive preventive measures to ensure safe, reliable and resilient financial systems. Digital payments have helped to boost economic efficiency and financial inclusion, but have also created a greater vulnerability to cyber threats, financial fraud, and data security risks. As a result, governments, financial regulators, payment service providers, and technology companies have taken several measures in the legal, technological, and institutional fields to improve the security of digital payment infrastructure and boost public trust in digital financial transactions. [13]

Role of Central Banks and Financial Regulators

Central banks and financial regulators are important in ensuring the safety, stability and integrity of digital payment systems. The Reserve Bank of India (RBI) is responsible for regulating payment and settlement systems in India, under the Payment and Settlement Systems Act 2007, and the National Payments Corporation of India (NPCI) is responsible for managing payment and settlement systems for retail payments, such as Unified Payments Interface (UPI). Regulatory institutions set standards on how the payments system works, oversee payment services providers, provide guidelines on cybersecurity, oversee systemic risks, and encourage secure digital financial innovations. The systems are kept robust against new cyber risks through periodic regulations, risk analysis, and

compliance checks, all of which also build trust in digital financial services for customers [14], [15]

Security Standards and Fraud Prevention Technologies

Digital payment systems have several technical and regulatory protections that ensure their security. Financial institutions must follow Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to confirm customer identities, stop account creation fraud and identify unusual financial activity. Multi-factor authentication, end-to-end encryption, tokenisation, biometric verification and real-time transaction monitoring are additional layers of security for payment infrastructure. Artificial intelligence (AI) and machine learning have proven to be useful in fraud detection in recent years by analysing transaction patterns, detecting unusual behaviour, and providing early warnings of potentially fraudulent activity. The technologies enable faster and more accurate fraud detection and reduce the financial impact and increase the security of payments. [16]

Consumer Awareness and Cyber Hygiene

Technological protection cannot prevent digital payment fraud because many frauds are committed due to human error. Thus, the understanding of consumers is an integral part of digital payment security. Financial regulators, banks, and fintech firms periodically carry out awareness programmes to teach users about phishing, fake payment apps, QR code scams, OTP fraud, and safe banking methods online. Suspicious links, strong passwords, multi-factor authentication, banks mobile application updates and keeping confidential banking information safe are all elements consumers are encouraged to adopt in good cyber hygiene. Enhanced digital literacy along with responsible user behaviour substantially decreases the risk of successful cyber-related financial crimes. [17]

Collaborative Approach to Payment Security

Digital financial crimes can only be prevented through collaboration between banks, fintech firms, central banks, law enforcement and cybersecurity firms. Financial institutions exchange threat intelligence, establish common fraud monitoring platforms and share information on incidents to track new threats. Digital financial crimes are being investigated by law enforcement and cybersecurity organizations help with technical expertise, vulnerability assessments, and threat intelligence, enhancing payment security. The role of public-private partnerships and international cooperation in the fight against cross-border cybercrime, in the fight against money laundering, and in the development of a common approach to cybersecurity has grown in significance. This joint governance fosters the

resilience of digital payment systems and contributes to the ongoing development of secure and trustworthy digital economies. [18]

LITERATURE REVIEW

(Leelavathi & Chandramohan, 2026) [19] In India's effort to become less cash-dependent and more digitally enabled, mobile payments have become an essential part of digital transactions. By permitting seamless transactions via a variety of digital platforms and mobile applications, the Indian payment ecosystem has been revolutionised by the widespread availability of smartphones and internet services. Due to the many advantages they provide to consumers, businesses, and the government, mobile payments have grown in popularity. With mobile payment apps being widely utilised for daily transactions, India has developed into one of the top digital payment marketplaces in the world. This study looks at how mobile payments have grown in India since 2016 and investigates the elements that have made them the most popular form of digital payment. Additionally, it examines the main forces behind the swift growth of mobile payments in the nation.

(Laxman et al., 2025) [20] examines the trends in academic research on online payment fraud, financial crime, and digital payment fraud using a thorough methodology that incorporates topic mapping, co-occurrence network analysis, and author cooperation networks. Growth rate, publication source, and author relationships in the retrieved field of study were all included in the results. According to the survey, the majority of research concentrated on topics like blockchain technology, artificial intelligence, digital signatures, credit card fraud, and so on. Another drawback of bibliometric study is its subjective character. The knowledge acquired from these studies can be applied by the managerial level to conduct awareness and training campaigns, invest in technologies that discourage fraud, and measure risk. Financial institutions can reduce fraudulent digital payment activities by using strategies and technology that adhere to current regulations and legislation. This improves payment security, which increases client retention and satisfaction.

(Singh & Agarwal, 2025) [21] determine and analyse the fundamental causes of digital payment forgeries, compare the perspectives of victims and non-victims, assess countermeasures, and evaluate the government's involvement in fraud prevention. The results show that the main causes of fraud are low awareness, cybersecurity flaws, financial illiteracy, and technical complexity. While non-

victims draw attention to cybersecurity vulnerabilities and sluggish investigations, victims emphasise financial illiteracy and technological complexity. The most successful countermeasures were found to be awareness and education, followed by stringent laws and security intelligence. New technologies, such as network tokenisation and sound wave authentication, were thought to be less successful. In order to improve the security of digital payments, "the report recommends AI-driven fraud detection, biometric authentication, cybersecurity frameworks, and fraud information sharing". These tactics necessitate a multi-stakeholder approach encompassing consumers, financial institutions, and regulators.

(Chandel & Chandel, 2025) [22] uses the Theory of Planned Behaviour (TPB), a well-known paradigm for comprehending technology adoption and personal decision-making, to investigate the factors influencing the adoption of digital payments. This research is particularly well-suited to TPB, as it elucidates the ways in which "attitudes, subjective norms, and perceived behavioural control (PBC)" influence an individual's intention to employ new technologies. The study intends to comprehend how these goals lead to increased financial inclusion among marginalised people by investigating these elements. The main conclusions show that attitudes about PBC and digital payment systems have a large influence on the desire to utilise these systems, but subjective standards have no bearing. Furthermore, financial inclusion is substantially predicted by behavioural intention, and this link is further strengthened by trust's mediating function. Increased confidence in digital financial services is essential for the advancement of financial inclusion in India, according to the results. Policymakers, financial service providers, and tech developers seeking to build more efficient strategies to boost digital payment acceptance and narrow financial access gaps in India's impoverished areas would find these findings particularly important. Despite its focus on India, the study has broader implications for emerging economies facing challenges with "digital infrastructure, trust, and financial inclusion". In nations with comparable socioeconomic and technological characteristics, the behavioural drivers that have been emphasised, particularly the importance of trust, can assist in the development of digital finance strategies.

(Sivasubramaniyan et al., 2025) [23] The study used a descriptive and causal research approach to investigate how digital payments contribute to Chennai's economic growth. A questionnaire was used to gather primary data from fifty Chennai-based consumers and businesspeople. According to

the report, most respondents believe that digital payments have a beneficial impact on economic growth. The necessity of enhancing security features and user confidence in digital payments is highlighted by the fact that almost half of the respondents trust digital payments, while a sizable minority are still sceptical. According to the report, there is broad agreement that digital platforms play a major role in linking urban and rural economic activity, promoting more equitable growth in Chennai's outskirts, and that small businesses and street sellers are using payments more frequently. The future of digital payments in Chennai is anticipated to be significantly shaped by UPIs, with contactless and mobile wallets also playing a significant role. Overall, the study's conclusions show that digital payments are highly preferred in Chennai.

(Wiwoho et al., 2022) [24] aims to provide a legislative framework to stop FinTech from being abused for financial crime in Indonesia and to detect the potential for digital payment usage for financial crime. This kind of study is known as legal research. A statutory comparative approach was the research methodology employed. Both main and secondary legal texts were utilised. Techniques for qualitative data analysis have been used to analyse the results. The study's findings demonstrate that FinTech digital payments have been employed in a number of terrorist financing instances as an online funding source. In this sense, a thorough legal framework is required through the creation of the Law on FinTech in order to preserve "the integrity of the financial system" and bolster the government's control functions.

(Gangadhar, 2026) [25] By enabling an effective and dependable payment system that satisfies the demands of companies, governmental organisations, and the general public, digital payments in India play a critical role in promoting economic progress. By improving "transparency, efficiency, and financial inclusion, digital banking platforms and electronic payment technologies" have drastically changed the financial transaction environment during the last ten years. The Reserve Bank of India (RBI) annual reports, statistical publications, and transaction statistics from "the National Payments Corporation of India (NPCI)" were the sources of the data. The research evaluates the structural development of digital banking, with particular reference to "the Unified Payments Interface (UPI)", using trend analysis tools and Compound Annual Growth Rate (CAGR). The results show that the number and value of digital transactions have significantly increased, especially through UPI. The report also outlines major obstacles to the

sustainability and inclusivity of digital banking in India and examines several forms of digital payments.

CONCLUSION

Digital payment systems have proven to be a key element of modern economies, in enhancing the efficiency of payment transactions, in fostering financial inclusion and in facilitating the growth of digital commerce and formal economic activities. The introduction of innovations like UPI, mobile wallets, internet banking and QR-based payments have played a significant role in improving economic growth by making it easier and faster to access financial services, lowering transaction costs, and making financial transactions more transparent. The digitalization of financial services has also led to an increased prevalence of financial crimes enabled by technology, such as phishing, identity theft, payment fraud and money laundering, undermining consumers' confidence and the stability of the financial system. To overcome these challenges, there needs to be comprehensive regulatory supervision, implementation of KYC and AML protocols, high-tech fraud detection systems, and ongoing consumer awareness campaigns. In addition, central bank cooperation is vital with financial institutions, fintech firms, cybersecurity firms, and authorities in order to improve payment security and counter rapidly changing cyber threats. A secure, resilient and inclusive digital payment system will continue to be an essential pillar towards sustainable economic growth and reduce the risks of digital financial transactions.

REFERENCES

- [1] D. S. S. Yendigeri, "The Evolution of Payment System in India: From Cash to Digital Wallets," *J. Emerg. Technol. Innov. Res.*, vol. 5, no. 5, pp. 2016–2018, 2018.
- [2] M. Saha and D. R. Thakkar, "Digital Payment Systems and Data Protection: Challenges and Risk Mitigation in Indian Commerce," *Int. J. Innov. Sci. Eng. Manag.*, vol. 5, no. 1, pp. 40–47, 2026, doi: 10.69968/ijisem.2026v5Si140-47.
- [3] D. S. J. Ghadge, "Digital Payment Systems Research: A Review of Empirical Studies," *Int. J. Innov. Sci. Eng. Manag.*, vol. 5, no. 1, pp. 90–96, 2026, doi: 10.69968/ijisem.2026v5i190-96.
- [4] N. Jindal, "The Evolution of Digital Payments and its Impact on the Economy," *Res. Arch. Rising Sch.*, pp. 1–13, 2023.
- [5] P. S. Lakshmi, "Impact of Digital Payments on the Indian Economy," *Int. J. Bus. Econ. Manag. Res.*, vol. 12, no. 4, pp. 1–14, 2021.
- [6] A. M. Shahen and M. F. Sharaf, "The Role of Digital Payment Technologies in Promoting Financial Inclusion: A Systematic Literature Review," *FinTech*, vol. 4, no. 59, pp. 1–18, 2025.
- [7] R. Ly and B. Ly, "Digital payment systems in an emerging economy," *Comput. Hum. Behav. Reports*, vol. 16, p. 100517, 2024, doi: 10.1016/j.chbr.2024.100517.
- [8] M. G. M. Hajare, P. (Dr. . S. S. Dhanawade, P. P. Kajale, P. B. Chavan, and P. A. Kadam, "A STUDY ON BENEFITS OF DIGITAL PAYMENTS," *J. Emerg. Technol. Innov. Res.*, vol. 12, no. 12, pp. 409–417, 2025.
- [9] M. Kakkar, L. N. Yadava, D. M. A. A. Directorate, and D. M. A. Associate, "Role of digital payment in the growth of MSMEs Sector," *Indian J. Econ. Bus.*, vol. 20, no. 1, pp. 885–891, 2021.
- [10] G. CHAUHAN and G. Kaur, "The Growth of Digital Payments In India," 2026.
- [11] S. Jain, A. A. Mishra, and J. P. Sahu, "The Economics of Digital Payments: A Systematic Literature Review and Future Research Agenda," *J. Econ. Surv. Surv.*, pp. 1–19, 2026, doi: 10.1111/joes.70068.
- [12] N. Mandavi, H. S. Bhatia, and O. P. Gupta, "UPI REVOLUTION IN INDIA: EXAMINING THE GROWTH AND TRANSFORMATION OF THE DIGITAL PAYMENT ECOSYSTEM," *Int. J. Res. Commer. Manag. Stud.*, vol. 8, no. 04, pp. 21–33, 2026.
- [13] V. R. Duvalla, "Real-time fraud detection in digital payments: Leveraging AI and behavioral analytics," *World J. Adv. Res. Rev.*, vol. 26, no. 2, pp. 1372–1380, 2025.
- [14] R. Chowdhury and D. S. A. Kumar, "IMPACT OF RBI REGULATIONS ON DIGITAL PAYMENT ADOPTION AND CONSUMER TRUST IN INDIA," *J. Nov. Res. Innov. Dev.*, vol. 4, no. 4, 2026.
- [15] G. RANJAN and D. S. SHARMA, "UPI as Public Digital Infrastructure: Re-thinking Regulatory Models under the Payment and Settlement Systems Act, 2007," *Int. J. Law Manag. Humanit.*, vol. 9, no. 2, pp. 4088–4105, 2026.
- [16] A. B. Rusman, "Strengthening Know Your Customer (KYC) and Anti-Money Laundering (AML) Policies in the Fintech Industry to Prevent Money Laundering Crimes," *J. WORLD Sci.*, vol. 4, no. 7, pp. 871–881, 2025.

- [17] C. YADAV and P. C. D'Souza, "Impact of Digital Payment Systems on Consumer Behaviour," 2026.
- [18] H. S. SHAREEKA and D. G. R. V, "LEGAL FRAMEWORK GOVERNING DIGITAL PAYMENT SYSTEMS AND E-COMMERCE TRANSACTIONS," *White Black Leg. Law J.*, vol. 2, no. 16, 2024.
- [19] G. Leelavathi and D. B. P. Chandramohan, "MOBILE PAYMENTS DRIVING THE GROWTH OF DIGITAL PAYMENTS IN INDIA," *IJDDT*, vol. 16, no. 60, 2026, doi: 10.25258/ijddt.16.60s.9.
- [20] V. Laxman, N. Ramesh, S. K. J. Prakash, and R. Aluvala, "Emerging threats in digital payment and financial crime: A bibliometric review," *J. Digit. Econ.*, vol. 3, pp. 205–222, 2025, doi: 10.1016/j.jdec.2025.04.002.
- [21] A. K. Singh and P. K. K. Agarwal, "AN OVERVIEW OF DIGITAL PAYMENT FRAUDS: CAUSES, CONSEQUENCES, AND COUNTERMEASURES," *J. Informatics Educ. Res.*, vol. 5, no. 1, pp. 2297–2311, 2025.
- [22] S. Chandel and S. Chandel, "The Role of Digital Payment Systems in Advancing Financial Inclusion in India," *Cureus J. Bus. Econ.*, 2025.
- [23] K. Sivasubramaniyan, M. T. Raman, and G. Surendar, "ROLE OF DIGITAL PAYMENTS IN DRIVING ECONOMIC GROWTH IN CHENNAI," *Int. J. Eng. Technol. Manag. Res.*, vol. 12, no. 9, pp. 21–41, 2025, doi: 10.29121/ijetmr.v12.i9.2025.1675.
- [24] J. Wiwoho, D. B. Kharisma, and D. T. K. Wardhono, "FINANCIAL CRIME IN DIGITAL PAYMENTS," *J. Cent. Bank. Law Institutions*, vol. 1, no. 1, pp. 47–70, 2022, doi: 10.21098/jcli.v1i1.7.
- [25] K. Gangadhar, "Digital payments in India: Benefits, Trends, Growth analysis, Challenges and future prospects –A Descriptive Study," *Int. J. Res. Anal. Rev.*, vol. 13, no. 1, pp. 70–77, 2026.