PAHAL HORIZON
An International Research Journal
Homepage: www.pahalhorizon.com

Security Awareness And Challenges In The Use Of E-Payment Systems For E-Commerce

Ms. Shivani Jain [1] Dr.Raju Thomas [2]
[1]Research Scholar, Department of Commerce, Applied Business Economics, St. John's College, Agra
[2]Associate Professor and Head, Department of Applied Business Economics, St. John's College, Agra

ABSTRACT

The increasing integration of e-commerce into everyday economic activities has led to a substantial rise in the use of electronic payment systems. Digital payment modes such as debit and credit cards, mobile wallets, Unified Payments Interface (UPI), and internet banking have simplified online transactions by offering speed, convenience, and ease of access. However, alongside these benefits, concerns related to security and user awareness have emerged as significant issues influencing the effective use of e-payment systems in e-commerce. Growing instances of cyber fraud, data breaches, and unauthorized access to financial information have raised apprehensions among users, thereby affecting their confidence in digital payment platforms.

The present paper seeks to examine security awareness related to e-payment systems and to discuss the major challenges associated with their use in the e-commerce environment. The study is based on secondary data collected from scholarly articles, regulatory reports, government publications, and other reliable sources related to digital payments and online commerce. The paper provides an analytical discussion of key security challenges, such as phishing attacks, identity theft, misuse of personal data, and technological vulnerabilities that impact user trust and perception towards e-payment systems. In addition, the importance of digital literacy and awareness of safe transaction practices in reducing security risks is highlighted.

The paper also emphasizes the need for improving security awareness among users to promote safer usage of e-payment systems. It discusses the role of financial institutions, e-commerce platforms, and regulatory

bodies in strengthening security mechanisms and implementing awareness initiatives aimed at educating users about secure digital payment practices. The study concludes by emphasizing that enhancing user awareness and addressing security-related challenges are essential for fostering trust and ensuring the sustainable growth of e-payment systems within the e-commerce ecosystem.

*Keyword***:** E-payment systems, E-commerce, Security awareness, Digital payments, Cyber security.

1. INTRODUCTION

Global economic activity has been profoundly altered by the digital revolution, especially in the domains of banking, financial services, and commerce. By facilitating online shopping and digital financial transactions, the rise of e-commerce platforms has opened up new company and consumer options. By enabling customers to send money electronically without requiring actual cash, e-payment systems are essential to these transactions.

Over the past ten years, electronic payment systems have been increasingly popular in India. Online transactions now frequently employ digital payment platforms such as digital wallets, debit and credit cards, internet banking, and the Unified Payments Interface (UPI). Across retail payment platforms, the Reserve Bank of India's reports demonstrate the steady rise in digital transaction volumes. In the same way, the National Payments Corporation of India's innovations have greatly increased the efficiency and accessibility of digital payment systems.

Digital payment methods are convenient, but as online transactions become more common, new cybersecurity issues have emerged. Through fraudulent operations like phishing assaults, identity theft, phone payment gateways, and unauthorized access to financial accounts, cybercriminals frequently take advantage of flaws in online payment procedures. These risks could undermine consumer confidence in online transactions and hinder the expansion of e-commerce sites.

As a result, user security knowledge becomes crucial for safeguarding customers from online fraud and guaranteeing secure online transactions. Users who are aware of safe payment procedures are less likely to fall prey to financial scams. Maintaining confidence in online financial institutions and fostering the expansion of digital commerce requires raising security awareness and enhancing digital payment protections.

Achieving the larger national goal of creating a technologically advanced and inclusive economy also depends on ensuring safe digital payment systems. Enhancing payment infrastructure and raising cybersecurity awareness would support Viksit Bharat @2047's long-term development goal, which prioritises equitable and sustainable economic transformation.

2. LITERATURE REVIEW

Oliveira, Thomas, and Baptista (2018) examined the factors influencing mobile payment adoption and concluded that perceived security and trust significantly affect consumer acceptance of digital payment technologies. Their study highlighted that users are more likely to adopt electronic payment systems when they believe their financial information is adequately protected.

Singh and Srivastava (2021) analyzed consumer behaviour toward digital payment platforms and found that security concerns strongly influence user satisfaction and continued usage of online payment systems. Their research suggested that improving security mechanisms can enhance consumer confidence in digital transactions.

Gupta and Arora (2019) investigated the growth of digital payment systems in India and identified technological infrastructure, regulatory policies, and consumer trust as key determinants of digital payment adoption. The study emphasized that consumer perception of security plays an important role in the expansion of electronic payment systems.
Kumar and Malhotra (2022) examined cyber fraud risks in online financial transactions and found that phishing attacks and identity theft are among the most common threats faced by digital payment users. The authors recommended strengthening cybersecurity awareness programs to reduce vulnerability to online financial fraud.

Zhao and Bacao (2020) also highlighted that perceived risk influences the adoption of mobile payment technologies. Their research suggested that improving security frameworks and user awareness can increase consumer trust and encourage wider adoption of digital payment platforms.
Sharma (2020) argues that digital literacy significantly influences safe transaction behaviour among online shoppers. Consumers with higher awareness levels are more capable of identifying fraudulent payment links, suspicious websites, and phishing attempts. Conversely, limited knowledge about cybersecurity practices increases exposure to financial fraud during e-commerce transactions.

TABLE 1: SUMMARY OF LITERATURE REVIEW

S. No.	Author(s) & Year	Focus of Study	Key Findings
1	Oliveira, Thomas & Baptista (2018)	Adoption of mobile payment technologies	The study found that perceived security and user trust significantly influence the adoption of mobile payment systems.
2	Zhao & Bacao (2020)	Factors affecting mobile payment usage	Results indicated that perceived risk and trust are major determinants influencing consumer acceptance of digital payments.
3	Singh & Srivastava (2021)	Consumer behavior towards digital payments	The study highlighted that security concerns and ease of use play a crucial role in encouraging the use of digital payment platforms.
4	Gupta & Arora (2019)	Growth of digital payments in India	Findings showed that technological infrastructure and regulatory support are key drivers of digital payment adoption.
5	Kumar & Malhotra (2022)	Cyber fraud in digital payment systems	The research identified phishing attacks and identity theft as major threats affecting digital payment security.
6	Sharma & Singh (2020)	Digital payment awareness among consumers	The study emphasized that digital literacy and awareness significantly reduce vulnerability to online payment fraud.
7	Patel & Rana (2021)	Security perception in online transactions	Findings suggested that stronger authentication systems increase consumer trust in online payment platforms.
8	Verma & Kapoor (2019)	Risk perception in e-commerce payments	The study indicated that perceived security risks often discourage users from engaging in online financial transactions.
9	Das & Agarwal (2022)	Digital payment adoption during digital transformation	Results showed that the growth of e-commerce has increased reliance on secure digital payment systems.
10	Mehta & Jain (2023)	Cybersecurity awareness in digital transactions	The study concluded that improving user awareness and regulatory safeguards can significantly reduce

			digital payment fraud.

Source: Author Compiled

In the Indian context, regulatory frameworks established by the Reserve Bank of India have strengthened authentication requirements, including two-factor verification and transaction alerts. However, despite regulatory interventions, reports of card-not-present fraud, fake refund scams, and OTP-based deception continue to surface. This highlights a persistent gap between regulatory measures and user-level awareness.

The above studies highlight that security concerns, perceived risk, and consumer awareness play a crucial role in determining the adoption and safe usage of e-payment systems. Although previous research has examined digital payment adoption and technological infrastructure, limited attention has been given to security awareness in the context of e-commerce transactions. This study, therefore, attempts to analyze security challenges and awareness related to the use of e-payment systems in online commerce.

3. RESEARCH GAP

Although several studies have examined the adoption of digital payment technologies, limited research specifically focuses on security awareness in the context of e-commerce transactions. Existing literature mainly emphasizes technological adoption and infrastructure development rather than the role of consumer awareness in preventing digital payment fraud.

Therefore, the present study attempts to address this gap by analyzing the challenges associated with digital payment security and the importance of consumer awareness in ensuring safe e-commerce transactions.

4. OBJECTIVES OF THE STUDY

- To examine the level of security awareness among users of e-payment systems in e-commerce transactions.
- To identify the major security challenges associated with digital payment systems.
- To analyze the impact of cybersecurity awareness on safe digital payment usage.
- To understand the role of secure digital payment infrastructure in supporting digital economic development.

5. RESEARCH METHODOLOGY

The present study is based on secondary data analysis. Information has been collected from academic research articles, institutional reports, and digital payment statistics related to e-commerce transactions. Major sources of information include reports published by the Reserve Bank of India and the National Payments Corporation of India, along with relevant scholarly literature and industry publications.
The study adopts a descriptive and analytical research design. Data collected from secondary sources has been analysed to identify major cybersecurity threats in digital payment systems and to evaluate the importance of consumer awareness in preventing online payment fraud.

6. E-PAYMENT SYSTEMS USED IN E-COMMERCE

Electronic payment systems enable online financial transactions between buyers and sellers without the use of physical currency. The rapid development of digital technologies has resulted in the emergence of various payment methods that facilitate secure and convenient online transactions.

TABLE 2: COMMON E-PAYMENT METHODS USED IN E-COMMERCE

E-Payment Method	Description	Security Concerns
UPI	Real-time bank-to-bank payment system	Phishing requests, fraudulent payment links
Debit/Credit Cards	Card-based electronic payments for online transactions	Card-not-present fraud
Net Banking	Direct banking authentication for payments	Fake banking websites
Digital Wallets	App-based electronic wallets	OTP misuse and account hacking

Source: Compiled by the researcher from secondary digital payment studies.

7. SECURITY CHALLENGES IN E-PAYMENT SYSTEMS

The rapid integration of e-payment systems into e-commerce platforms has enhanced transactional efficiency but has simultaneously exposed consumers and businesses to evolving cybersecurity threats. The digital nature of online transactions, combined with the exchange of sensitive financial information, creates multiple points of vulnerability. The following are the major security challenges associated with the use of e-payment systems in e-commerce environments.

1. Phishing Attacks

Phishing remains one of the most prevalent threats in e-commerce transactions. Cybercriminals often send fraudulent emails, SMS

messages, or advertisements impersonating legitimate e-commerce platforms. These messages typically contain malicious links directing users to counterfeit websites that closely resemble authentic platforms. Unsuspecting consumers may enter card details, login credentials, or OTPs, leading to financial loss.

Phishing attacks are particularly common during festive seasons and promotional sales when online traffic increases significantly. The urgency created by limited-time discounts makes consumers more susceptible to deception.

2. Identity Theft

Identity theft occurs when cybercriminals gain unauthorized access to personal or financial information and use it to perform fraudulent transactions. This type of cybercrime can lead to significant financial loss for victims.

3. Fake Payment Gateways

During the checkout process, users are redirected to payment gateways to complete transactions. Fraudsters exploit this stage by creating fake payment interfaces that mimic genuine gateways. Once users input their financial details, the information is captured and misused.

Although secure gateways employ encryption technologies such as SSL certificates, consumers may fail to verify website authenticity. This highlights the importance of security awareness in identifying secure transaction indicators such as HTTPS protocols and verified domain names.

4. Card-Not-Present Fraud

In e-commerce transactions, physical card verification is absent. This makes card-not-present fraud a significant challenge. Stolen card details obtained through data breaches or phishing are used to conduct unauthorized online purchases. Since the cardholder is not physically present during the transaction, detection becomes more complex.

Even with two-factor authentication systems regulated by the Reserve Bank of India, fraudsters may exploit social engineering techniques to obtain OTPs from victims,

5. Malware and Spyware Attacks

Malicious software installed on devices can monitor user activity and capture sensitive financial information, increasing the risk of digital payment fraud.

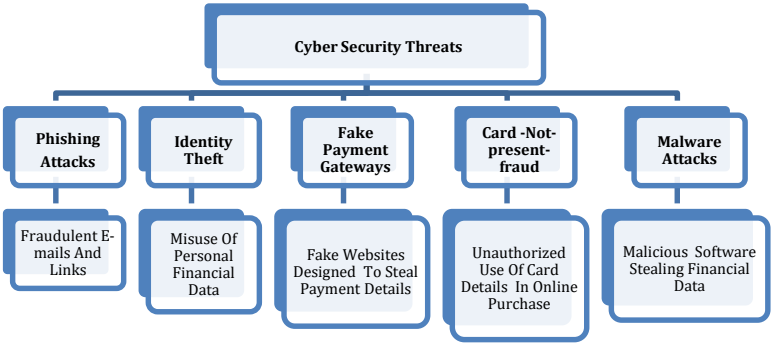
6. Refund and Chargeback Fraud

Fraudulent refund claims and chargeback abuse have emerged as operational challenges in e-commerce. In some cases, fraudsters manipulate return policies to claim refunds after receiving goods. Conversely, consumers may also become victims of fake refund messages requesting payment verification details.
These fraudulent activities undermine trust in digital payment ecosystems and increase financial risk for both merchants and consumers.

7 .Data Breaches of E-Commerce Platforms

Data breaches at e-commerce companies can expose large volumes of consumer information, including payment credentials. Even when payment processing is outsourced to secure gateways, vulnerabilities in platform databases may compromise stored data. Such incidents significantly erode consumer trust and may lead to long-term reputational damage for businesses.

FIGURE 1: MAJOR CYBER SECURITY THREATS AFFECTING E-PAYMENT SYSTEMS



Source: Developed by the researcher based on secondary literature.

8. ROLE OF SECURITY AWARENESS

Security awareness plays an essential role in preventing cyber fraud in digital payment systems. Users who follow safe digital practices are less likely to become victims of financial cybercrime.
Important security practices include:

- Avoiding sharing OTPs and passwords
- Verifying website authenticity before making payments
- Avoiding suspicious payment links
- Using secure devices for online transactions
- Reporting fraudulent transactions immediately

Improving digital literacy and cyber security awareness can significantly enhance consumer confidence in digital payment systems.

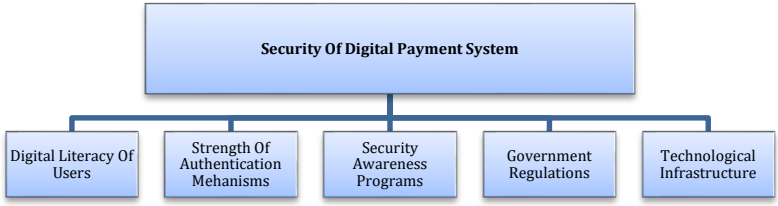


FIGURE 2: KEY FACTORS INFLUENCING THE SECURITY OF DIGITAL PAYMENT SYSTEMS
Source: Conceptual framework developed by the researcher.

9. GROWTH OF DIGITAL PAYMENT SYSTEMS IN INDIA

The rapid expansion of digital infrastructure in India has significantly accelerated the adoption of electronic payment systems. Over the past decade, increasing smartphone penetration, affordable internet services, and government initiatives promoting digital transactions have transformed the payment ecosystem. Digital platforms such as Unified Payments Interface (UPI), mobile banking applications, and digital wallets have simplified financial transactions and improved accessibility for consumers across both urban and semi-urban regions.

According to reports published by the Reserve Bank of India, digital payment volumes in India have witnessed consistent growth in recent years. The introduction of interoperable payment platforms and real-time settlement systems has enhanced transaction efficiency and convenience. Similarly, innovations introduced by the National Payments Corporation of India have played a crucial role in strengthening India's digital payment infrastructure.

The growth of e-commerce platforms has further contributed to the increased use of electronic payment methods. Online marketplaces require secure and efficient payment mechanisms to facilitate transactions between buyers and sellers. As a result, digital payment services have become an integral part of the modern e-commerce ecosystem.

However, while the expansion of digital payments provides significant benefits, it also creates new challenges related to cybersecurity and consumer protection. Ensuring a secure payment infrastructure and promoting awareness among users are essential to maintain trust in digital transactions.

TABLE 3: MAJOR DIGITAL PAYMENT PLATFORMS USED IN INDIA

Payment Platform	Key Features	Usage in E-commerce
UPI	Instant bank-to-bank transfer	Widely used for mobile payments
Debit Cards	Direct bank account deduction	Common for online purchases
Credit Cards	Deferred payment facility	Used for high-value transactions

Digital Wallets	Prepaid digital payment apps	Popular for quick small payments

Source: Developed by the researcher.

10 IMPACT OF SECURITY CHALLENGES ON CONSUMER TRUST

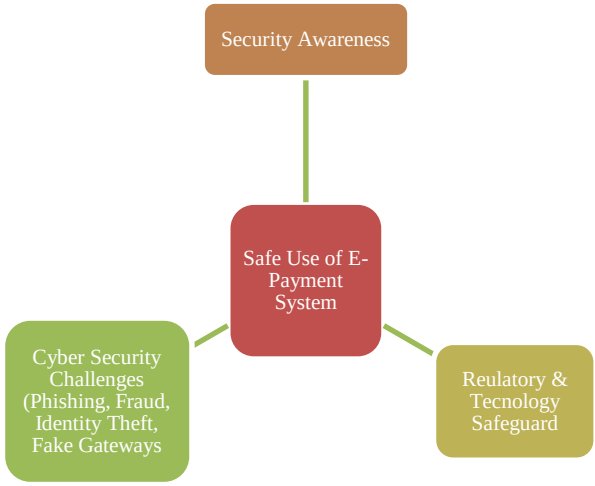
Consumer trust plays a vital role in the adoption and continued use of digital payment systems. When users perceive online payment systems as secure and reliable, they are more likely to engage in e-commerce transactions. However, increasing incidents of cyber fraud can negatively affect consumer confidence and discourage individuals from using digital payment platforms.

Cybersecurity threats such as phishing attacks, unauthorized access to financial accounts, and fake payment gateways often target users who lack awareness about secure online practices. In many cases, users unknowingly share confidential information such as OTPs, passwords, or card details with fraudulent entities. Such incidents may result in financial losses and reduce the credibility of digital payment systems.

Studies suggest that consumers who possess higher levels of digital literacy and cybersecurity awareness are less likely to become victims of online fraud. Therefore, strengthening security education programs and improving user awareness can significantly reduce cyber risks associated with digital payment systems.

Financial institutions and regulatory authorities have also introduced several protective measures, such as two-factor authentication, secure payment gateways, and transaction alerts. These mechanisms aim to improve the safety of digital transactions and protect users from unauthorized financial activities.

FIGURE 3: CONCEPTUAL RESEARCH MODEL OF SECURITY AWARENESS AND CHALLENGES IN E-PAYMENT SYSTEMS.



Source: Developed by the researcher.

11 EXPLANATION OF CONCEPTUAL FRAMEWORK.

The conceptual framework of this study explains the relationship between security awareness, cybersecurity challenges, and the safe use of e-payment systems in e-commerce transactions. With the rapid expansion of digital commerce, electronic payment platforms have become an essential medium for conducting financial transactions. However, the increasing dependence on digital payment technologies has also exposed users to various cybersecurity threats such as phishing attacks, identity theft, fraudulent payment links, and fake online payment gateways.

In this framework, security awareness among users is considered a key factor influencing the safe usage of e-payment systems. Consumers who possess adequate knowledge about secure digital practices, such as protecting personal credentials and verifying payment platforms, are less likely to become victims of cyber fraud. At the same time, cybersecurity challenges act as risk factors that may negatively affect consumer trust in online payment systems.

Regulatory safeguards, technological security mechanisms, and user awareness initiatives help mitigate these risks and strengthen the safety of digital transactions. Therefore, improving cyber security awareness and strengthening digital payment protection measures are essential for

ensuring secure e-commerce transactions and supporting the development of India's digital economy in line with the vision of Viksit Bharat @2047.

12. POLICY IMPLICATIONS

Strengthening the security of digital payment systems is essential not only for protecting individual consumers but also for ensuring the sustainable growth of India's digital economy. As e-commerce continues to expand, maintaining consumer trust in electronic payment mechanisms becomes increasingly important.

- Several policy measures can support this objective:
- Expanding national cyber security awareness campaigns
- Enhancing digital literacy programs for rural and semi-urban populations
- Implementing stronger authentication technologies in payment platforms
- Strengthening regulatory monitoring of digital payment service providers
- Encouraging collaboration between financial institutions and cyber security agencies

These initiatives can help create a safer digital payment environment and encourage wider participation in electronic commerce. Secure digital payment systems will contribute significantly to financial inclusion and economic participation across different socio-economic groups.
Such improvements are aligned with the broader national objective of building a technologically advanced and inclusive economy envisioned under Viksit Bharat @2047.

13. CONCLUSION

The rapid expansion of digital commerce has increased the importance of secure electronic payment systems. Although e-payment technologies provide convenience and efficiency, they also introduce cyber security risks that must be addressed to ensure safe financial transactions.
Improving consumer awareness, strengthening cyber security infrastructure, and implementing effective regulatory frameworks can help minimize online financial fraud. Secure digital payment ecosystems will support the continued growth of e-commerce and contribute to inclusive economic development in India.

Strengthening digital payment security will also support the national development vision of Viksit Bharat @2047, which emphasizes sustainable digital transformation and inclusive economic growth

14. REFERENCE

- Oliveira, T., Thomas, M., & Baptista, G. (2018). Mobile payment adoption. *Computers in Human Behavior*.
- Singh, N., & Srivastava, S. (2021). Consumer behavior and digital payments. *Journal of Retailing and Consumer Services*.
- Gupta, S., & Arora, N. (2019). Digital payment adoption in India. *International Journal of Bank Marketing*.
- Kumar, V., & Malhotra, A. (2022). Cyber fraud and digital payment security. *Journal of Financial Crime*.
- Zhao, Y., & Bacao, F. (2020). Factors influencing mobile payment adoption. *Telematics and Informatics*.
- Reserve Bank of India. (2024). *Annual report 2023–24*. Reserve Bank of India.
- National Payments Corporation of India. (2024). *UPI product statistics*. National Payments Corporation of India.