Analyzing Security Risks and User Awareness in Digital Payments

Mr. Sudhir Soman[1], Aditi Atul Sathe[2]
[1]Assistant Professor, Department of Computer Science Tilak Maharashtra Vidyapeeth, Pune
[2]Student of MCA, TMV

Abstract—**Digital payment systems have rapidly transformed the global financial landscape, enabling faster, more efficient, and convenient transactions. The increasing adoption of digital payment platforms has been influenced by factors such as technological advancements, the rise of e-commerce, government initiatives promoting cashless economies, and growing smartphone penetration. However, this growth has also brought about several security concerns, including risks related to data breaches, identity theft, phishing, malware attacks, and transaction fraud. Addressing these security challenges is crucial for building trust among users and ensuring the continued success of digital payment systems. This research paper explores the security concerns in digital payment systems by reviewing existing literature, analyzing data from a primary survey, and discussing the major threats and vulnerabilities faced by users and service providers. The study also provides recommendations to enhance digital payment security and highlights the importance of user awareness and regulatory measures. This survey is conducted through a questionnaire of 30 respondents.**

Index Terms—**digital payment, security concerns, data breach, identity theft, malware, transaction fraud, user awareness, digital payment systems.**

I. INTRODUCTION

The world has seen a significant shift toward digital payment systems in recent years. People and businesses have moved from traditional cash transactions to electronic payments because it is faster, easier, and more efficient. The growth of digital payments has been influenced by several factors. First, technological advancements such as the internet, smartphones, and secure networks have made it possible for people to make payments from anywhere at any time. Second, the rise of e-commerce has encouraged the use of online payment systems. Third, governments in many countries have promoted cashless transactions to increase transparency and reduce corruption. Fourth, the COVID-19 pandemic further accelerated the adoption of digital payment platforms because people wanted to avoid touching cash. Despite these positive factors, digital payments also face several challenges. One of the major challenges is security. Many people worry about the safety of their personal and financial information when using digital payment systems. Cybercriminals often target these systems to steal money and data. Other challenges include lack of awareness among users, technical issues like server downtime, and digital illiteracy in some regions. This research paper aims to study the security concerns in digital payment systems, understand the various threats involved, and suggest possible solutions to improve security and user trust.

Factors Influencing the Growth of Digital Payment

1. Increased internet penetration.
2. Advancement in mobile technology.
3. Government initiatives for cashless societies.
4. Pandemic-driven demand for contactless payments.
5. Growth of e-commerce.
6. Improved financial inclusion through digital platforms.

Various Challenges Involved in Digital Payment

1. Risk of data breaches and cyber-attacks.
2. Lack of strong authentication processes.
3. Privacy concerns and misuse of personal data.
4. Low user awareness about security risks.
5. Regulatory and compliance issues.
6. Technical vulnerabilities in payment platforms.

The following sections provided a comprehensive overview of the evolution of digital payments, examined the primary security risks, discussed the challenges in implementing secure systems, and reviewed possible solutions and recommendations for improving digital payment security.

II. REVIEW OF LITERATURE

Sharma and Gupta (2019): Sharma and Gupta (2019) studied the growth of digital payment systems in India and highlighted the security risks faced by users. They found that while digital payments have made transactions easier, users are often exposed to threats like phishing attacks and identity theft. The study suggested that increasing user awareness and implementing strong authentication methods can help reduce these risks.

Lee et al. (2020): Lee et al. (2020) examined the adoption of digital payment platforms in Southeast Asia and discussed the impact of cyberattacks on user confidence. The research showed that incidents of data breaches and transaction fraud have led to a lack of trust among users. The authors recommended continuous monitoring of payment systems and the use of advanced encryption technologies to overcome these challenges.

Patel (2021): Patel (2021) focused on the security challenges in mobile payment applications. The study identified malware attacks and software vulnerabilities as major concerns for users. It also emphasized the need for regular updates and educating users about safe practices to protect themselves from security threats.

III. OBJECTIVES OF THE STUDY

1. To identify the major security concerns in digital payment systems.
2. To analyse user awareness regarding digital payment security.
3. To examine the types of threats and vulnerabilities in digital payment platforms.
4. To suggest measures for improving security in digital payment transactions.

IV. SOURCES OF INFORMATION

Primary Sources: The main primary source was a survey conducted among digital payment users. The survey included questions related to their experiences with digital payment security, awareness of risks, and opinions on improving safety. Secondary Sources: The study also used information from published journals, research articles, and online reports related to digital payment security to support the analysis and provide context.

V. STATEMENT OF THE PROBLEM

Digital payment systems, while convenient and efficient, are exposed to various security threats that can compromise user data and financial assets. This research aimed to understand these security issues and propose solutions to address them.

VI. HYPOTHESIS

Higher user awareness of digital payment security features is associated with a lower incidence of security breaches and a greater level of trust in digital payment systems.

This hypothesis is grounded in the assumption that users who are more informed about risks and security practices are better equipped to prevent and respond to threats, thereby reducing their exposure to fraud, phishing, and unauthorized access (Singh & Kaur, 2021; Oser et al., 2020).

VII. SCOPE AND LIMITATIONS OF THE STUDY

Scope: This research focuses on the interplay between security risks and user awareness in digital payment systems, primarily examining consumer-facing platforms accessed via smartphones and computers. The analysis integrates findings from a primary survey of urban users and synthesizes insights from recent scholarly work on token-based payments, smart contract security, and human-centered risk frameworks.

The study's scope is defined by the following parameters:

1. Concentrates on common digital payment modalities, such as mobile wallets, online banking, and programmable payment platforms.
2. Addresses the most prevalent security threats: phishing, data breaches, malware, and transaction fraud.
3. Examines user awareness, education, and behaviour in relation to digital payment security.
4. Excludes point-of-sale (POS) devices and payment modalities not widely adopted in consumer digital contexts.

This focused approach allows for an in-depth analysis of security risks and user behaviours most relevant to contemporary digital payment users, providing actionable insights for service providers, regulators, and end users.

VIII. LIMITATIONS

1. The survey sample was limited to users from urban areas, which may not represent the experiences of rural users.
2. The research focused mainly on digital payment systems used on smartphones and computers, excluding other methods like point-of-sale (POS) devices.
3. The study was conducted within a specific time frame, so it may not capture new types of security threats that could arise in the future.

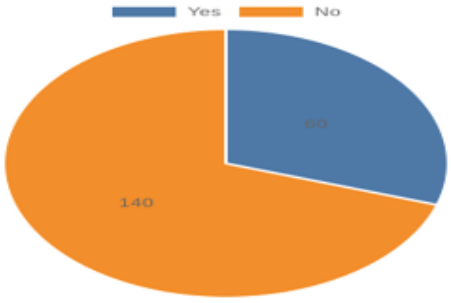
IX. DATA ANALYSIS AND INTERPRETATION

A survey was conducted with 200 digital payment users. The following nine questions were asked to understand their experiences and concerns regarding digital payment security. Each question is followed by a table representing user responses, a short analysis, a pie chart, and its interpretation.

1: Have you ever faced any security issues while using digital payment systems?

Particulars	Number of Users	Percentage
Yes	60	30%
No	140	70%

Analysis: 30% of surveyed users reported experiencing security issues with digital payment systems, while 70% did not face any such problems. This indicates that a significant portion of users have encountered security concerns.

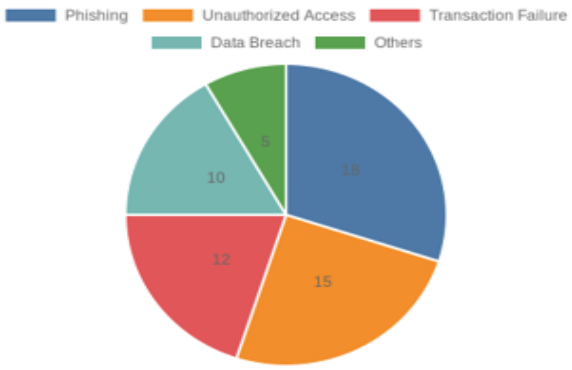


Interpretation: Most users have not faced security problems, but a notable minority (30%) have encountered issues, showing that security is still a concern for some users.

2: What type of security issue have you faced while using digital payments?

Security Issue	Number of Users	Percentage (of total 60)
Phishing	18	30%
Unauthorized Access	15	25%
Transaction Failure	12	20%
Data Breach	10	17%

Analysis: Phishing was the most common issue faced by users, followed by unauthorized access and transaction failures. Data breaches and other issues were also reported, but less frequently.

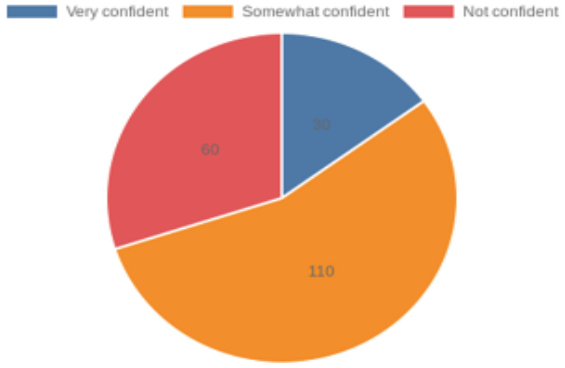


Interpretation: -
Phishing and unauthorized access are the most prevalent security issues, highlighting the need for better awareness and stronger authentication methods.

3: How confident are you in the security of digital payment systems?

Level of Confidence	Number of Users	Percentage
Very confident	30	15%
Somewhat confident	110	55%
Not confident	60	30%

Analysis: Most users (55%) felt somewhat confident in digital payment security, while 30% were not confident and only 15% felt very confident.

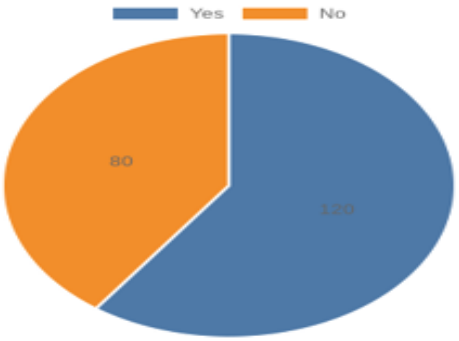


Interpretation: There is general trust in digital payments, but a significant number of users still lack full confidence in the security measures provided by service providers.

4: Are you aware of the security features (like OTP, encryption) used in digital payment systems?

Particulars	Number of Users	Percentage
Yes	120	60%
No	80	40%

Analysis:
60% of users were aware of security features in digital payment systems, while 40% were not. This suggests a need for more user education on security measures.

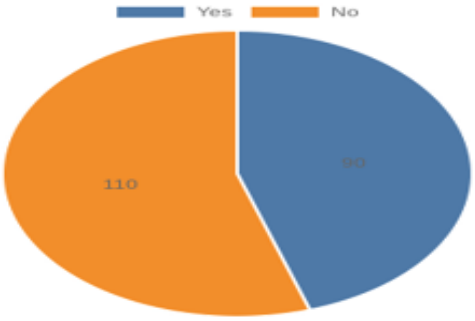


Interpretation:
While most users know about security features, a large percentage lack this knowledge, making them more vulnerable to security threats.

5: Have you ever updated your digital payment app to improve security?

Particulars	Number of Users	Percentage
Yes	90	45%
No	110	55%

Analysis: More than half of users (55%) did not update their payment app regularly, which could expose them to security risks.

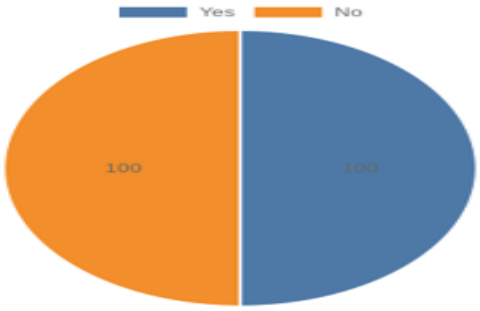


Interpretation: User negligence in updating apps is a potential risk factor in digital payment security.

6: Do you use strong passwords or biometric authentication for digital payments?

Particulars	Number of Users	Percentage
Yes	100	50%
No	100	50%

Analysis: Half of the users used strong authentication methods, while the other half did not, indicating a gap in secure usage practices.

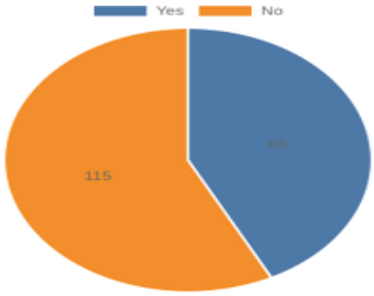


Interpretation: There is an equal split between users who follow secure practices and those who do not, highlighting the need for more awareness.

7: Have you received any suspicious messages or calls related to digital payments?

Particulars	Number of Users	Percentage
Yes	85	42.5%
No	115	57.5%

Analysis: About 42.5% of users reported receiving suspicious messages or calls, indicating that social engineering attacks are common.

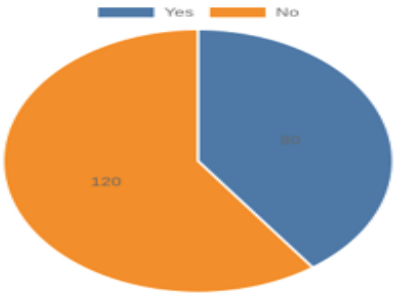


Interpretation: A significant number of users have been targeted by social engineering attempts, underlining the importance of user vigilance.

8: Do you think digital payment service providers do enough to ensure security?

Particulars	Number of Users	Percentage
Yes	80	40%
No	120	60%

Analysis:
Most users (60%) felt that service providers do not do enough to ensure security, showing a gap between user expectations and current practices.

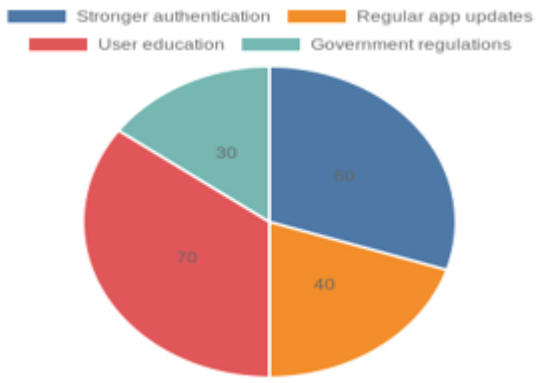


Interpretation: There is dissatisfaction among users regarding the security efforts of digital payment companies.

9: What do you think is the most effective way to improve digital payment security?

Suggestion	Number of Users	Percentage
Stronger authentication	60	30%
Regular app updates	40	20%
User education	70	35%
Government regulations	30	15%

Analysis: User education was considered the most effective way to improve security, followed by stronger authentication methods.



Interpretation: Most users believe that educating people about security is the best solution, showing that awareness is key to reducing security risks.

X. FINDINGS AND CONCLUSION

Findings:

1. A significant portion of users have faced security issues such as phishing, unauthorized access, and transaction failures.
2. User awareness regarding digital payment security features is moderate, but a large percentage still lack knowledge and do not follow safe practices.
3. Many users do not update their payment apps regularly or use strong authentication methods.
4. There is dissatisfaction with the security measures provided by digital payment service providers.
5. User education is seen as the most important step to improve digital payment security.

Conclusion: Digital payment systems have made financial transactions faster, easier, and more convenient. However, they also bring new security challenges like phishing, unauthorized access, and data breaches. This research showed that many users are still unaware of basic security practices and do not update their apps regularly. While some users trust digital payment systems, others remain concerned about their safety. The study suggests that raising user awareness, implementing stronger security measures, and enforcing regulations can help reduce risks and build trust in digital payment systems. Everyone—service providers, users, and regulators—must work together to make digital payments safer for all.

XI. SUGGESTIONS AND RECOMMENDATIONS

Suggestions:

1. Service providers should invest in user education campaigns to raise awareness about security features and safe usage practices.
2. Digital payment apps should prompt users to update regularly and make updates mandatory for critical security fixes.
3. Stronger authentication methods, such as biometrics and two-factor authentication, should be widely implemented.
4. Regulatory authorities should enforce minimum security standards for all digital payment service providers.
5. Users should be encouraged to use unique and strong passwords, and avoid sharing personal information with unknown sources.

Recommendations:

1)Enhance User Education: Service providers and regulators should implement ongoing education campaigns that demystify security features and promote best practices. User-friendly guides, interactive tutorials, and in-app prompts can empower users to recognize threats and respond effectively (Oser et al., 2020; Singh & Kaur, 2021).

2)Mandate Regular Updates and Strong Authentication: Digital payment platforms should enforce mandatory updates for critical security patches and widely adopt multi-factor authentication, including biometrics and OTPs. Automated reminders can reduce user negligence (Patel, 2021).

3)Adopt Human-Centered Risk Communication: Inspired by frameworks developed in IoT and AI contexts, digital payment systems should present clear, context-sensitive risk information and obtain in-context consent for sensitive transactions. Transparency in data usage and privacy implications fosters greater trust (Chen et al., 2025; Oser et al., 2020).

4)Implement Programmable Security Controls: Utilizing modular smart contract templates and token-based payment streams can automate security checks and enforce compliance, reducing the attack surface and operational errors (Meng & Feng, 2024; Goodell, 2024).

5)Strengthen Regulatory Oversight: Regulators should establish and enforce minimum security standards across all digital payment providers, including requirements for encryption, fraud monitoring, and incident reporting (World Bank, 2020).

6)Promote User Agency and Control: Systems should offer granular privacy settings and clear options for users to control their data, reflecting principles of contextual integrity and privacy calculus (Chen et al., 2025).

REFERENCES

[1] Lee, S., Tan, J., & Wong, K. (2020). User confidence and cybersecurity in digital payment adoption. Journal of Financial Technology, 5(2), 87–102.
[2] Patel, M. (2021). Security challenges in mobile payment applications. International Journal of Information Security, 20(4), 233–242.
[3] Sharma, A., & Gupta, R. (2019). Security risks in the growth of digital payment systems. International Journal of Computer Science and Technology, 10(1), 45–51.
[4] Kumar, V., & Sinha, R. (2019). Cybersecurity challenges in digital financial transactions. International Journal of Computer Applications, 182(10), 25–30.
[5] McKinsey & Company. (2021). The future of digital payments: Opportunities and risks. McKinsey Global Institute Report. Retrieved from https://www.mckinsey.com
[6] National Payments Corporation of India (NPCI). (2022). UPI security guidelines and user awareness. NPCI Publications. Retrieved from https://www.npci.org.in
[7] PwC. (2020). Securing the digital wallet: Strategies for safer transactions. PricewaterhouseCoopers Report. Retrieved from https://www.pwc.com
[8] Reserve Bank of India (RBI). (2021). Report on trends and progress in digital payments in India. RBI Annual Report. Retrieved from https://www.rbi.org.in
[9] Singh, A., & Kaur, P. (2021). User awareness and trust in mobile payment applications. Journal of Information Security, 12(3), 145–156.
[10] World Bank. (2020). Digital financial services: Security and risk management. World Bank Publications. Retrieved from https://www.worldbank.org