ISSN: (P) 2319 – 8915 and (E) 2583-4282

TRENDS, SECURITY, TRUST AND INTENTION TO USE DIGITAL PAYMENTS IN INDIA – A LITERATURE REVIEW

Heena Shrivastava, Dr. Manish Sidhpuria and Dr. Sagar Gaur

ABSTRACT

The relationship between finance and technology with internet use triggered the emergence of digital payment technologies. Such technological innovation in the e-payment industry is the foundation for financial inclusion. Digital payments have been emerging payment systems across the globe in recent years, and they are a beneficial and convenient way to receive and make payments digitally. The government's quest towards a cashless economy has created a robust regulatory framework to safeguard the safety and security of digital transactions. The RBI is India's major regulatory organization supervising digital payments and ensuring that all digital payments follow through with the compliances designed.

This research study explores how the trends, digital payment mode has been used efficiently worldwide. How soundly developed and developing nations impending their economies with the help of digital payment usage. This research paper aims to study the present trends of the digital market along with its associated security features. The study tries to compile a comprehensive literature review on digital payment technologies. It also studies the security aspects and various threats of e-payment systems by collecting different literature reviews on security aspects. In summary, reviewing past studies reveals some loopholes and benefits of digital payment and future perspectives of the digital payment industries.

The present study is a descriptive study to determine what shoppers consider when buying food and grocery products from different retail formats. Data are collected using a structured questionnaire from the respondents drawn from the Surat district of the South Gujarat region using a non-probability convenience sampling technique.

In most nations, including India, security is the paramount concern for digital payment. Trust and privacy of users and information from third parties are crucial. The availability and reliability of digital Infrastructure, including internet connectivity, mobile networks, and payment processing systems, is crucial for digital payment services in framing the user's intention towards digital payments.

Key words: :Digital payment, Security, Trust, Intention

I. INTRODUCTION

The world has been quickly advancing and has undergone digital transformation. Online and digital payments are among the prime factors shaping the present and future of e-payment industries. Various businesses are leveraging digital payment systems to expand trade and adopt technology in day-to-day life.

Contactless payments are one of such digital payment trends that will be proliferating in the year 2024. Contactless payments allow customers to wave their smartphones or cards across the reader and make payments. This method is nearly instant easier and more convenient than cash or swinging a card. As we continue navigating the digital age, mobile payments, cashless payments, blockchain technology and AI-driven fraud detention are among the top trends revolutionizing the future of the payment processing industry.

A significant boost for the digital payment system came during the period of demonetization of currency by the government of India in 2017 and the COVID-19 outbreaks in 2019. The programme's main objective is to use cashless, paperless and faceless transactions in the emerging economy. This year, 91 billion digital payments have been made. The methods for digital payments are more secure than traditional check payments because multiple layers of encryption and authenticated possessions protect them. Such methods help to reduce the risk of account takeover and other types of financial crime. The data has revealed that India currently has around 350 million online transacting users across the country, primarily involved in day-to-day transactions like e-commerce payments, shopping, travel and hospitality and OTT, and the number is set to double by 2030.

Regulatory Authorities of Digital Payment:

Various regulatory authorities in India control the digital payment Industry, including the RBI, the NPCI and the Ministry of Electronics and Information Technology. The RBI regulates and supervises the digital payment system in India. It offers rules and regulations concerning digital payment system security, risk management, client protection, and other factors. The NPCI (National Payment Corporation of India) includes UPI, Immediate payment service, and the Baharat bill payment system.

The Ministry of Electronics and Information Technology (MEITY) is in charge of developing the country's digital Infrastructure, which includes digital literacy, e-governance and digital payments. It collaborates with other regulatory bodies and industry stakeholders to promote the efficient adoption of the digital payment system in India.

Most digital payments in India, including those made using mobile wallet applications, prepaid & debit cards, and online platforms, are governed under the Payment and Settlement Act 2007. The Act creates frameworks for oversight and monitoring digital payment service providers. It also authorizes and supervises payment system operations and issues regulations to ensure the safety and efficiency of the digital payments industry.

To maintain cardholder data security during digital transactions, merchants in India must ensure the payment card Industry data security standards. It should follow and establish a secure network, monitor and test security systems regularly and maintain an information security policy. Merchants must also follow the RBI's KYC standards, which require verifying the names and addresses of their clients before onboarding them. These policies and procedures should help build the customer's confidence in data security and provide information.

Compliances of Digital Payment:

The Reserve Bank of India (RBI) has published detailed guidelines to strengthen India's digital payment architecture and provide transparency, security trust, control and proper compliance to safeguard and help achieve its goal of a "less cash" economy.

All digital payments in India, including those made using mobile wallets, prepaid cards, and online platforms, are governed under the Payment and Settlement Act 2007. The act creates frameworks for oversight and monitoring digital payment service providers. It also authorizes and supervises payment system operations and issues regulations to ensure the safety and efficiency of the digital payments industry.

To maintain cardholder data security during digital transactions, merchants in India must ensure the payment card Industry data security standards. It should follow and establish a secure network, monitor and test security systems regularly

and maintain an information security policy. Merchants must also follow the RBI's KYC standards, which require verifying the names and addresses of their clients before onboarding them. These policies and procedures should help build the customer's confidence in data security and provide information.

Here are a few examples of digital payment fraud in India:

- The Paytm Fraud Case (2018): Scammers tricked Paytm consumers by pretending to offer reward schemes in one of India's largest digital payment frauds. They would call people pretending to be Paytm personnel, coercing them into installing remote access applications that would give them access to their phones and enable them to take control of their victims' Paytm accounts.
- The PNB Scam (2018): Unauthorised operations totalling more than $1.8 billion (INR 13,000 crore) were a part of the Punjab National Bank (PNB) scam. Bank staff fraudulently issued fraudulent Letters of Undertaking (LoUs) to Nirav Modi's enterprises, which needed more appropriate collateral or due diligence. Payments for foreign trade were made more accessible with the help of the finances.
- The SBI Card Fraud (2019): Phishing scammers sent false emails claiming to be from the State Bank of India (SBI), fooling several SBI credit cardholders. The emails asked recipients to disclose confidential data and verify their KYC (Know Your Customer) details; this information was later utilised for unauthorised transactions.
- The Yes Bank Fraud (2020): Using its mobile banking app, Yes Bank saw an instance of a digital payment scam. A flaw in the software allowed fraudsters to generate UPI IDs without users' permission and withdraw money from their accounts. The Bank gave customers refunds, guaranteeing their money would remain secure.
- The Google Pay Fraud (2020): Scammers carried out Unauthorised activities using the UPI-based Google Pay technology. Users lost money due to hackers tricking them into disclosing their OTP or UPI PIN, which was then utilised to commit fraud.
- The significant data breach that affected millions of customers' Bank and private data occurred at the well-known digital wallet and payment service

MobiKwik in 2021. It has been revealed that the compromised data, namely card details and KYC information, was offered for trade on the dark web.

- The Coinsecure Bitcoin Scam of 2018: Millions of dollars' worth of bitcoins were lost due to a significant security failure at Coinsecure, an Indian cryptocurrency exchange. The stock exchange claimed that the fraud resulted from an insider, which prompted impacted users to file lawsuits against the fraud and demand the damages caused.

These instances highlight the difficulties and dangers of using digital payments in India, such as insider fraud, phishing schemes, data breaches, and banking system weaknesses. To tackle these concerns, authorities, banks, companies that provide payment services, and users must work together to improve security protocols, increase public awareness, and put anti-fraud solid systems in place.

Matter of Non-Compliance by Financial Institutes

In India, security and privacy are critical features of digital payments. The Reserve Bank of India has issued guidelines for digital payments security and the company and merchant bank partners should adhere to follow the respective compliance guidelines timely.

Paytm Payments Bank

Paytm Payment Bank of non-compliance matter here the RBI stated that after allowing the business enough time to address its non-compliance issues, the decision was reached to prohibit Paytm Payments Bank from taking fresh deposits and topping up Paytm wallet from February 29, 2023, later deadline has been extended by RBI to March 15th. Paytm's stock has fallen by more than 42 percent in three days, and investors lost Rs. 20500 crores. The company's shares have dropped dramatically by more than 60% in the last six months. The Reserve Bank of India's enforcement of stringent regulatory actions against Paytm Payments Bank, which cited persistent non-compliance issues, caused the most significant decline in Paytm's stock price. Investors and Paytm consumers are worried as the RBI has ordered the payments bank to cease a few crucial operations as of March 1. Furthermore, Paytm offered clarification in response to media reports implying that Paytm had been the target of a case filed by the Enforcement Directorate (ED) for breaking FEMA regulations.

RBI slaps penalties totalling Rs 10.34 cr on Citibank, Bank of Baroda, and IOB

The Reserve Bank of India (RBI) also fined Indian Overseas Bank, Bank of Baroda, and Citibank a combined Rs. 10.34 crores for their non-compliance. The public sector lender Indian Overseas Bank, with its headquarters in Chennai, received a punishment of Rs 1 crore for violating multiple regulatory regulations, while the state-owned Bank of Baroda was penalised Rs 4.34 crore. At Rs 5 crore, Citibank incurred the highest penalty.

<Figure-1>, <Figure 2> and <Figure 3>

Context:

As we have seen in the above graph, the Unified Payments Interface (UPI) recorded over 10 billion transactions in August; this is a historic milestone.

Consistent Month-on-Month Growth:

- UPI saw 9.96 billion transactions in July, indicating a steady month-on-month growth.
- UPI averaged around 330 million transactions daily in August, potentially reaching 10.5 billion monthly transactions.

Expected Transaction Value Record:

- The transaction value for August is estimated to surpass July's record of Rs 15.33 lakh crore, settling around Rs 15.4 – 15.6 lakh crores.

UPI's Evolution and Growth Factors:

- UPI has evolved from a person-to-person money transfer system to a significant driver of commerce, with 57 per cent of transactions now being merchant transactions.
- QR code adoption by millions of merchants, along with popular UPI apps like PhonePe, Google Pay, Paytm, Cred, and Amazon Pay, contributed to this rapid growth.
- Factors like demonetization and the pandemic accelerated the digitization of payments in India, supported by proactive policies.

National Payments Corporation of India (NPCI's) Ambitious Target:

- NPCI aims to achieve 30 billion transactions per month, equivalent to one billion transactions daily, in the next two to three years.
- NPCI is an umbrella organization for operating retail payments and settlement systems in India, and it is an initiative of the Reserve Bank of

India (RBI) and the Indian Banks' Association (IBA) under the provisions of the Payment and Settlement Systems Act, 2007.

Market Share of UPI Applications

Before the Paytm crisis, the two US-owned players – Walmart's PhonePe and Google's local payments services – controlled, on an average, 80-85% of UPI volumes of transactions every month. National Payment Corporation of India (NPCI) data as of December 2023 shows PhonePe had a 46% share in UPI volumes, followed by Google Pay at 36% and Paytm Payments Bank at 13%.

Volume of Transaction in Digital Payment

In the financial year 2023, there were over 83 billion UPI transactions worth about 139 trillion Indian rupees across India. The number of transactions was estimated to rise up to over 379 billion in the financial year 2027 in the country. Unified Payments Interface (UPI) was introduced by the National Payments Corporation of India (NPCI) in 2016 and facilitates inter-bank transactions.

II. REVIEW OF LITERATURE

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
Abu Sayed Md Mostafizur Rahaman et al. 2022 - Bangladesh	Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems	Authentication Integrity, Availability, Confidentiality and Accountability to assure Cyber Security	Perceived Security	• The cyber security issues of mobile payment applications to defend against cyber-threats are a significant apprehension of the software developer and user. A group of technologies and methods schemed to defend computers, software, networks, and data from being impaired by various types of cyber-attacks or unauthorized entrance are comprehended as Cyber security • Financial service organizations want their apps to be protected from fraudulent activities.
Nor Aslily Sarkam et. al. 2022 – Malaysia	Attitudes, Security, and Perceived Ease of Use Influence the Consumers' Decision to use an E-payment System	Convenience Efficiency, Trust, Security, Traceability, Perceived Usefulness	Perceived Ease of Use & Consumers' Intention	• The findings reveals direct effect suggested that attitude is the most critical aspect in consumers' intention to use e-payment systems. • The indirect effect results revealed that perceived ease indirectly affects towards consumers' intention to use EPS. • Perceived ease of use has a mediating effect between efficiency and perceived usefulness
Thanh D. Nguyen &	E-Payment Continuance	Transaction Procedures,	Perceived Security,	• Perceived trust impacts majorly on context of continuance Usage in e-payment usage.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
Quynh N. T. Tran 2022 - Vietnam	Usage: The Roles of Perceived Trust and Perceived Security	Technical Protections, Security Statement, Personal Past Exp-erience, Perceived Security, Perceived Trust	Perceived Trust	• Hands-on experience gained through use and training may help reduce uncertainty and create favorable user perceptions. • Perceived security negatively affects e-payment continuance usage. • Investing in the latest and modern technology to ensure the security of e-payment transactions.
Neha Priya & Jawed Ahmed 2021 –India	A Survey on Digital Payments Security: Recent Trends and Future Opportunities	Security Applications Data Intelligence	Security	• Security applications under this head are promising research themes, especially fraud detection. • The digital payments' growth challenges combined with growth assurance factors have scope of future IS security research. • Areas where research contribution is low, such as cyber forensics and data intelligence, are potential research opportunities.
Rasistia W. Primadineska & Syayyidah M. Jannah, 2021 – Indonesia	Perceived Security and Trust in Electronic Paym-ent Systems: How they affect the Decision to use EPS during Covid -19 Pandemic	Technical Protection	Perceived Security, Trust of EPS	• The results show that the presence of technical protection explicitly affects the perception users of security and trust significantly. • Security also dramatically affects an individual's confidence in the use of digital payment systems.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
				• Trust is the only one factor that influences the choice to use EPS.
Md. Arif Hassan, et. all, 2020 – Malaysia	A Review on Electronic Payments Security	Authorization Confidentiality , Integrity, Authentication and Non-repudiation	Efficiency	• The analysis of the selected studies shows several challenges and topics for future research, including those specifically related to using electronic payment systems to improve the security and interoperability of e-wallets and online payment system • However, providing security is a task that needs exhaustive evaluation and even more initiative than just using cryptographic mechanisms
Jiaxin Zhang, Yan Luximon and Yao Song, 2019 –PRC	The Role of Consumers' Per-ceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services	Perception of Customization Design, Perception of Feedback Design Conscientiousness	Perceived Security, Perceived Control, User Intention	• Perceived security is determining factor from the perspectives of customization design and feedback design, perceived control and conscientiousness, and revealed the strong relationship between perceived security and continuous use. • Perceived security also affects post-adoption behaviors, such as switching behaviors, advanced use, and recommended intention.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
M. Noor Ardiansa, Anis Chariri, and Indira Januarti, 2019	Empirical Study on Customer Perception of E-Commerce: Mediating Effect of Electronic Payment Security	Perceived Usefulness, Perceived Ease of Usefulness	Payment Security	• E-payment would increase a secure mechanism for sensitive information transmission (e.g., credit card or social security number) in the actual condition of system use. • Systems that can prove reliability and validity that are employed and give high accuracy from decision-making by optimization. • Consumer' purchase intentions influenced by understanding of ease of use and usefulness without association with the security aspects of payment.
Sandeep Dangol and Sandeep Kautish, 2019 – Nepal	IT Security Related Issues and Challenges in Electronic Payment System in Nepal: A Study From Customers Perspectives	Relevant Security Issue, Lack of Usability, Provider Issue, Lack of Security, Payment System Issue	Payment Gateway	• System of e-payment should be secure enough for the data that the customer transfers from the merchant to the appropriate payment gateway. • Most customers do not feel safe in the online payment world as there are too many problems and news related to data theft and breaches. In such cases, the payment gateway should secure its system and gain trust of its customers by implementing the flawless system. • Security and threats arise due to lack of proper advice to the users, lack of awareness & training, etc.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
				• 70% of the respondents think that the security threat susceptibility is due to user unawareness. It will not eliminate the vulnerabilities but will reduce them since the users are the ones who are affected.
Zuroni Md Jusoh Teng Yee Jing, 2019 – PRC	Perceived Security, Subjective norms, Self Efficacy Intention and Actual usage Towards E-Payment among UPM Students	Gender Perceived security Subjective norms Self-efficacy	Intention Actual usage	• Banking institutions should showcase their e-payment products and highlight the security features to boost the confidence level of consumers that their personal and financial information is well protected. • Bank branches can carry out demonstrations and tutorials to deliver quality information on the features of e-payment services, eliminate any misperceptions, ease navigation and boost confidence level of consumers when using e-payment.
Burhan Ul Islam Khan, 2017 – Malaysia	A Survey on E-Payment Systems: Elements, Adoption, Architecture,	Integrity, Confidentiality Availability	ICT Frameworks	• Security issues rely upon basic ICT frameworks that make liabilities in economic organizations, businesses and can possibly hurt clients. • Most recognized strategy for securing e-payments is utilizing cryptographic-based innovations, For Ex: digital signs these innovations lessen speed & proficiency and thus trade-off must be made

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
	Challenges and Security Concepts			between effectiveness and security features and encryption. • Study has also analyzed the EPS from an adaptability point of view to provide a better customer understanding and satisfaction.
P C Lai, 2016 – Malaysia	Design and Security Impact on Consumers' Intention to use Single Platform E-Payment	Perceived Usefulness Perceived Ease of Use	Authentication Integrity, Non-repudiation Confidentiality Reliability, Authorization	• The management needs to look into providing secured solutions with high security standards. • To reduce the perceptions of security single platform E-payment system suppliers can organize talk to educate consumers on safeguarding their E-payment transactions with the additional security and privacy features. • Security features will increase the consumers' trust and confidence leading to the intention to use a single Platform E-payment system.
Tamara Maaitah et. all, 2015 – UK	Review Study on the Security of Electronic Payment Systems	Integrity Authentication, Cheat avoidance and Allowance, Privacy	Intention Actual Usage	• The significance of Authorization and Significance encryption affect the perceived security of E-finance transactions. • These characteristics can enhance the perceptions of users that the web and online transactions, including E-Finance transactions, are safe, and inspire them to

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
		Transferability Payment Anonymity		use the online system and do financial transactions electronically.
Princewill Aigbe et. all, 2014 - Nigeria	Analysis of Security Issues in Electronic Payment Systems	Authentication to assure cyber security vulnerability confidentiality	E-Payment Security	• The study highlighted the application of the different authentication mechanisms and types in the categories of the electronic payments system. • Analysis reveals that electronic payment systems with involving two or more authentication factors is more secure, reduce fraud vulnerability, and boost users' confidence in using electronic payment systems.
Md. Atwah Al-ma'aitah, 2013 - Jordan	Security Concerns in E-Payment and the Law in Jordan	Integrity Authentication, Fraud prevention and tolerance, Privacy Divisibility, Transferability Payment anonymity	Intention Actual Usage	• Security and privacy are considered two critical elements in dealing with electronic transactions in general. • Lack of proper security shows that privacy will be the victim leads to the unwillingness of citizens to accept the idea of dealing with electronic commerce in general, and electronic payment specifically.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
Md. AL-ma'aitah and Abdallah Shatat, 2011-Malaysia	Empirical Study in the Security of Electronic Payment Systems	Authentication, Authorization, Privacy Encryption	Perceived Security	• Security features such as authorization and encryption are essential mechanisms to be present and practiced during E-Finance transactions.
Wahab Samsudin, 2011 – Jordan	The Influence of Perceived Privacy on Customer Loyalty in Mobile Phone Services:An Empirical Research in Jordan	Customer Loyalty, Customer Privacy	Perceived Privacy	• Concerning the factors influencing customer loyalty, the present research suggests that privacy is an important determinant. • Mobile phone service and security providers should strive to improve performance in their efforts to attain higher level of customer loyalty.
Linck, Kathrin et all, 2006 - Sweden	Security Issues in Mobile Payment from the Customer Viewpoint	Confidentiality Authentication Integrity Authorization Non-repudiation	Intention Actual Usage	Security is an essential condition. Fulfilling all essential conditions causes a customer to accept a mobile payment procedure as: • A usable method of payment in principle for acceptance into actual usage. • For security, essential conditions are to be found in the area of cost and convenience. • A payment procedure.

Sources And Country	Title of the Literature	Factor Influences	Mediating Factors	Major Outcomes of the Study
Theodosios Tsiakis & George Sthephanides, 2005 - Greece	The Concept of Security and Trust in Electronic Payments	Divisibility, Transferability, Double-spending prevention, Payment confidentiality, Payment anonymity, Payer un-traceability	Integrity, Authentication, Fraud prevention and Tolerance, Privacy	• Trust for secure transactions is accompanied with a significant amount of investments. • The Web of trust is based on pre-existing relationships (informal type) between parties and Certificate authority's e-reaction of relationship (formal method) achieved by means of Public Key Infrastructure (PKI).
France Belanger, Janine S. Hiller1, Wanda J. Smith, 2002 - USA	Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes	Perceived Usefulness, Perceived Ease of Use, Purchase Intention	Site Quality, , Site Trustworthiness, Importance of Security & Privacy Features	• Findings indicate that security features were most important to the consumer. • Security features were ranked as most important by the sample, with privacy and security seals and privacy and security statements all highly correlated; respondents indicate that requirements for one of these features on a Web site lead to a desire for the others. • It is also possible that users generally understand the concept of security better than privacy because it is more concrete concept.

III. RESEARCH BACKGROUND, STUDY DESING AND METHODOLOGY,

Rational of the Study:

The present research study tries to explain the digital payment trends in the Indian market, and most importantly, the paper covers major security threat issues associated with digital payments. The reason behind studying this topic is that the digital payments landscape in India is expected to grow in the upcoming years with profound changes along with new and updated technologies. India has a large population, a significant portion traditionally underserved by formal banking channels. Studying digital payments helps us understand how technology can bridge the gap and bring more people into the formal financial system. Today is the era of technologies and innovations where the economy rushes. The rapid pace of finance and technologies has led to the emergence of digital payment modes. Our present government is more focused on promoting digital payments as part of its Digital India campaign, as we have seen in the recent example of the G20 Summit, which India holds. With the gradation of smartphone technology, banking licenses to non-banking and private players have changed the payment system, which has now become fully digitalized. Digital payment is a vast area to study, including e-payment, card payment, e-wallet, UPI, Net banking, etc. So, in every single mode transaction via an electronic platform, there comes a concerning issue of security and trust with digital payments. Studying digital payments provides insights into consumer behaviour, preferences, and adoption patterns. This information is valuable for businesses, financial institutions, and policymakers in designing products and policies that meet the needs of consumers. It also provides financial stability by reducing the dependency on cash transactions. Studying digital payments provides insights into consumer behaviour, preferences, and adoption patterns. The study is also a beacon of information for businesses, financial institutions, and policymakers in designing products and policies that meet the needs of consumers.

The Objective of the study:

To review the literature regarding the current trends, security aspect, and trust regarding use of digital payments.

To review the intention to use digital payments.

Research Methodology:

To provide a systematic, transparent, and reproducible literature review of digital payment technologies, based on the diagram below, a process of study has been done.

IV.FINDINGS

After reviewing the research work of various authors, it is found that security is the paramount concern for digital payment. Cases like online fraud, phishing, malware, etc., significantly affect user intention. In parallel, the trust or privacy of users and information from third parties are crucial. The availability and reliability of digital infrastructure, including internet connectivity, mobile networks, and payment processing systems, are fundamental to the functioning of digital payment services. Inadequate infrastructure, particularly in rural and remote areas, can hinder adoption, and accessibility is also an essential consideration in framing the user's intention towards digital payments.

V. CONCLUSION

Digital payment has developed as a significant force in India's economy, fueled by the government's push towards a cashless economy and technology enhancement. With initiatives such as the Aadhar based banking, Bhim UPI, Bharat QR, and the adoption of digital wallets and e-payment in India, the usage of digital payments is likely to increase further. As per the literature review study here, we have seen that in India, people still hesitate to use digital mode due to the threats and security concerns, which is major because of the lack of sufficient knowledge, proper advice to the users, lack of awareness training, etc.

The Reserve Bank of India (RBI) gives the highest importance to security control; it will create an enhanced and enabling environment for customers to use digital payment products more safely and securely. Further study reveals that electronic payment systems with proper authentication mechanisms involving two or more authentication factors tend to be more secure, reduce fraud vulnerability, and boost users' confidence in digital payment systems. Concerning all these factors that influence customer loyalty, the present research paper suggests that security and privacy are essential determinants for the future growth of the digital payment system in India.

Challenges and Limitations:

The study reveals that despite the many benefits of moving from cash- and paper-based systems to digital payments, these challenges are roadblocks to digital transformation and must be addressed. These challenges are financial literacy, especially in rural and semi-urban areas, poverty, inadequate physical infrastructure like internet connectivity and POS terminals, especially in rural areas, and cyber security, which remains a significant concern for digital payments. Fraud, phishing, and cybersecurity breaches, especially among older or less tech-savvy individuals, include perception of customers, transaction charges, privacy protection, authenticity of information, trust, etc. Digital payments in India heavily rely on smartphones. The penetration of smartphones is increasing, but many still do not have access to smartphones, limiting their ability to make digital transactions. Transaction limits imposed by banks or payment service providers, especially for peer-to-peer transactions, are also a barrier, especially for large amounts of transactions. In India, the main reason for barricading the expansion is unequal access to technology, creating digital divides; rural areas face challenges in obtaining reliable and high-speed internet connectivity, limited digital access, and technology literacy. The result is the gap in digital transformation. Overall, while digital payments in India have made significant progress, addressing these limitations will be critical for further expansion and guaranteeing financial inclusion for all segments of society. It's essential for all stakeholders, including the government, regulators, financial institutions, and technology companies, to work in an organized way to overcome such challenges in future.

Limitation of the Study:

- The research paper is limited to digital payments' security, trust and intention issues.
- The study is based on the literature review, so the findings are limited majorly to the secondary data.
- Other demographic and physiological factors need to be addressed and impact can be measured.

Future Perspective:

The digital payments environment in India is likely to continue upward as more people adopt digital transactions in their daily routine lives. This growth may be

boosted by features such as increasing internet connectivity, the rise in usage of smartphones, and efforts to bring rural areas into the streamline of the digital era. NDA Government-led initiatives, such as the Pradhan Mantri Jan Dhan Yojana (PMJDY) and Unified Payments Interface (UPI), Rupay, Aadhaar Enabled Payment System (AEPS) and many such initiatives promoted financial inclusion and digital payments. Government policies and initiatives may further support the expansion of digital payment infrastructure.

Modern FinTech companies and traditional financial institutions may continue to invest in and adopt technological innovations. With the increasing volume of digital transactions, there is likely a heightened focus on improving the security of digital payment systems, implementing advanced authentication methods and strict cyber security measures to protect users' financial records.

A new face Artificial intelligence (AI) may play a more significant role in personalized financial services, fraud detection, and customer experience. Financial institutions and fintech companies may leverage these technologies to provide more efficient and personalized digital payment solutions.

Also, with international trade and collaborations increasing, there may be a growing demand for efficient cross-border payment solutions. Digital platforms offering seamless and cost-effective cross-border transactions could see increased adoption. We saw a change in the regulatory environment, which will continue to evolve to accommodate the changing landscape of digital payments. Regulatory bodies may introduce new guidelines to ensure consumer protection, fair competition, and the overall stability of the financial environment.

References

Akpojaro, P. A. (2014, December). Analysis of Security Issues in Electronic Payment Systems. *International Journal of Computer Applications, 108*(10), 10-14.

Al-ma'aitah, M. A. (2013). Security Concerns in E-payment and the Law in Jordan. *(IJACSA) International Journal of Advanced Computer Science and Applications, 4*(7), 179-183.

AL-Maaitah, T. A. (2015, September). Review Study on the Security of Electronic Payment Systems. *International Journal of Economics, Commerce and Management, 3*(9), 821-829.

C, L. P. (2016, September). Design and Security impact on consumers' intention to use single platform E-payment. *Interdisciplinary Information Sciences, 22*(1), 111-122.

France Belanger, J. S. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems, 11*(1), 245-270.

Iffath Tanjim Moon, M. S. (2022). Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems. *Journal of Computer and Communications, 10*(1), 103-129.

Jannah, R. W. (2021). Perceived Security and Trust in Electronic Payment Systems: How They Affect the Decision to Use EPS During the COVID-19 Pandemic. *Jurnal Manajemen Bisnis, 12*(2), 236-247.

Jiaxin Zhang, Y. L. (2019, December). The Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services. *Sustainability, 11*(1), 1-16.

Jing, Z. M. (2019, February). Perceived Security, Subjective Norm, Self-Efficacy, Intention, and, Actual Usage Towards E-Payment Among UPM Students. *Journal of Education and Social Sciences, 12*(2), 8-22.

Kautish, S. D. (2019, December). IT Security Related Issues and Challenges in Electronic Payment System in Nepal: A Study from Customer's Perspective. *LBEF Research Journal of Science, Technology and Management, 1*(2), 85-103.

Linck, K. a. (2006). Security Issues in Mobile Payment from the Customer Viewpoint. *14th European Conference on Information Systems (ECIS 2006)*, (pp. 1-11). Schweden.

M. Noor Ardiansah, A. C. (2019, September). Empirical Study on Customer Perception of E-Commerce: Mediating Effect of Electronic Payment Security. *Jurnal Dinamika Akuntansi, 11*(2), 122-131.

Md Arif Hassan, Z. S.-K. (2020). A Review on Electronic Payments Security. *Symmetry 2020*, 1-22.

Mohammad AL-ma'aitah, A. S. (2011). Empirical Study in the Security of Electronic Payment Systems. *International Journal of Computer Science*, 393-401.

Muddassir Masihuddin, B. U. (2017). A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian Journal of Science and Technology, 10*(20), 1-19.

Neha Priya, Jawed Ahmed (2021, August). A Survey on Digital Payments Security: Recent Trends and Future Opportunities. *International Journal of Computer Trends and Technology*, 69(8).26-34.

Nor Aslily Sarkam, N. F. (2022). Attitudes, Security, and Perceived Ease of Use Influence The Consumers' Decision to Use An E-payment System. *International Journal of Academic Resaerch in Business & Social Sciences, 12*(3), 357-368.

Samsudin Wahab, A. S. (2011, March). The Influence of Perceived Privacy on Customer Loyalty in Mobile Phone Services: An Empirical Research in Jordan. *IJCSI International Journal of Computer Science Issues, 8*(2), 45-52.

Theodosios Tsiakis, G. S. (2005). The concept of security and trust in electronic payments. *Computers & Security*, 10-15.

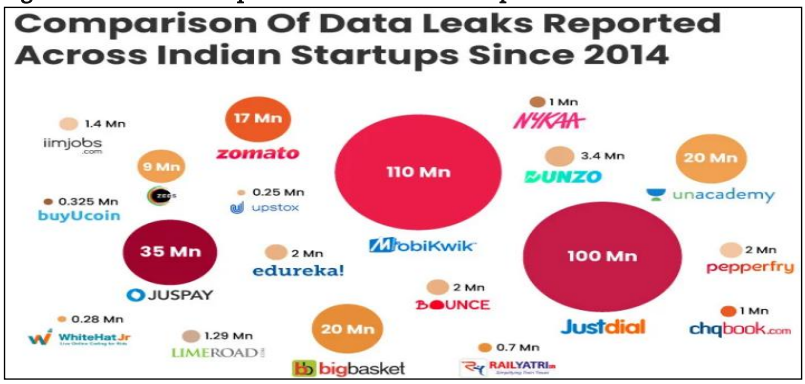
Tran, T. D. (2022). E-Payment Continuance Usage: The Roles of Perceived Trust & Security. *Springer*, 253-264.

Websites:

- https://pwonlyias.com/current-affairs/data-point-4/
- https://economictimes.indiatimes.com/tech/technology/paytm-crisis-upi-market-share-cap-rule-in-focus-leaders-may-corner-a-bigger-pie/articleshow/107406233.cms?from=mdr
- https://www.statista.com/statistics/1247111/india-number-of-upi transactions/#:~:text=In%20financial%20year%202023%2C%20there,year%202027%20in%20the%20country
- https://www.businesstoday.in/industry/banks/story/rbi-slaps-penalties-totalling-rs-1034-cr-on-citibank-bank-of-baroda-and-iob-407068-2023-11-24
- https://inc42.com/features/how-indian-govts-weak-stance-on-data-privacy-has-allowed-startups-run-leaky-ships/

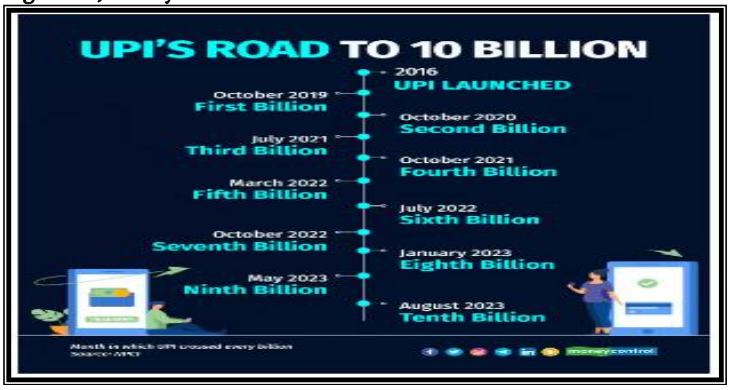
List of Figure

Figure 1: Data Leaks Reported Across India Startups Since 2014



Source:https://inc42.com/features/how-indian-govts-weak-stance-on-data-privacy-has-allowed-startups-run-leaky-ships/

Figure 2: Journey of 10 billion UPI Transactions



Source: https://pwonlyias.com/current-affairs/data-point-4/

Figure 3 Types of digital Payment

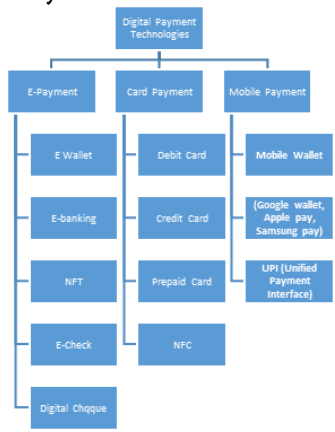
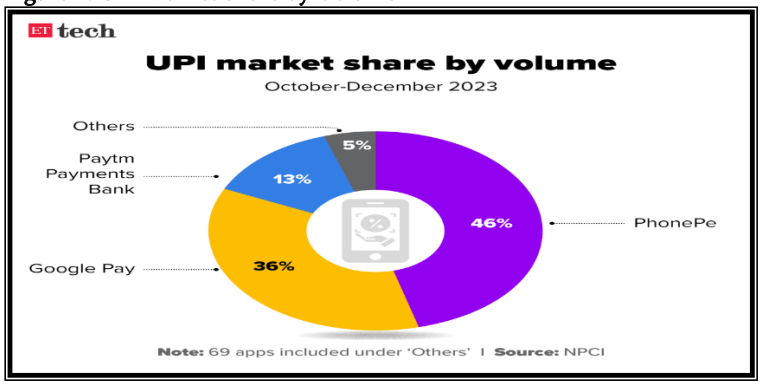
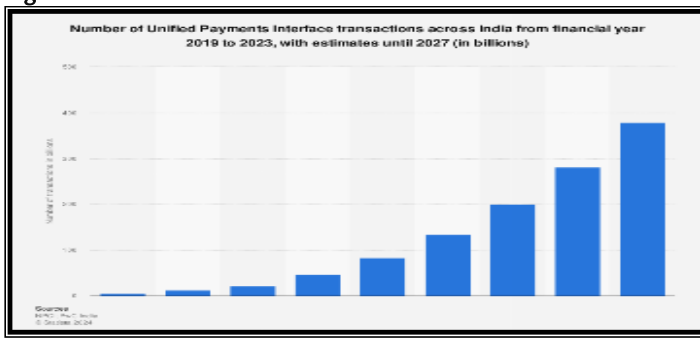


Figure 4: UPI Market Share by Volume



Source: https://economictimes.indiatimes.com/tech/technology/paytm-crisis-upi-market-share-cap-rule-in-focus-leaders-may-corner-a-bigger pie/articleshow/107406233.cms?from=mdr

Figure 5: Number of UPI transactions in India FY 2019-2027



Source: https://www.statista.com/statistics/1247111/india-number-of-upi transactions /#:~:text=In%20financial%20year%202023%2C%20there,year%202027%20in%20the%20country

Authors Profile

Miss Heena V. Shrivastava is a Ph.D. Research Scholar with 8 years of industrial experience. She holds an MBA (Finance), BBA, and has completed the Executive Programme of Company Secretary. She has published and presented more than 7 research papers in national and international journals and conferences. She has also completed certification programmes in Import–Export, NSE Financial Market (AMFI Advisory Module), and IRDA, and has actively participated in various academic development programmes.	
Dr. Manish V. Sidhpuria Professor & (HOD), Department of Business & Industrial Management, V. N. South Gujarat University, Surat. Dr. Sidhpuria has over 31 years of combined teaching and industry experience, including 8 years in the healthcare sector and more than 23 years in postgraduate management education, research, and consultancy. He has published over 50 research papers in reputed journals. His management cases have won prestigious awards at the Association of Indian Management Schools (First Prize – 2000; Third Prize – 2005). He has also received "Best Research Paper" awards at various conferences. He is the author of the book Retail Franchising published by Tata McGraw-Hill (India) and McGraw-Hill International (Philippines). Currently, he serves as the Coordinator of the MBA (Evening) programme for working executives.	
Dr. Sagar M. Gaur is an Assistant Professor at SDJ International College, Plasana, with 15 years of academic experience. He holds a Ph.D., M.Phil., and MBA (Marketing). He has published and presented more than 12 research papers in national and international journals and conferences. He is a co-author of three books in management subjects and has actively participated in various workshops, seminars, FDPs, and webinars.