E-Financial Sentinel: Navigating India's Digital Transaction Landscape

Conference Paper · November 2024

DOI: 10.1109/DELCON64804.2024.10866177

2 authors:

Subhra Prosun Paul
Chandigarh University
17 PUBLICATIONS **42** CITATIONS
SEE PROFILE

Dipayan Ghosh
Indian Institute of Technology Kanpur
6 PUBLICATIONS **0** CITATIONS
SEE PROFILE

E-Financial Sentinel: Navigating India's Digital Transaction Landscape

Subhra Prosun Paul
Department of Computer Science and Engineering
Uttara University
Uttara, Dhaka
subhra.phd.cu2021@gmail.com

Dipayan Ghosh
Department of Computer Science and Engineering
C3i Hub, IIT, Kanpur
Kanpur, India
dipayanghoshk@gmail.com

***Abstract*- The landscape of digital transactions in India is rapidly evolving, propelled by advancements in technology and the growing adoption of online payment methods. Payment gateways perform a critical role in enabling secure and seamless transactions between customers and merchants, enabling businesses to thrive in this dynamic ecosystem. This paper provides an overview of payment gateway functionality, key considerations for selecting providers, and steps to secure online money transactions effectively. It highlights the importance of encryption, authentication measures, and compliance with regulatory standards. Furthermore, it explores future trends such as biometric authentication, blockchain technology, and quantum-safe cryptography, which hold promise for enhancing transaction security. By embracing innovation and collaboration, payment gateway providers can mitigate cyber threats, foster trust, and propel India towards a cashless economy built on reliability and convenience. Continuous vigilance and adaptation are essential to navigate the evolving digital transaction landscape and unlock the full potential of India's digital economy.**

Keywords– Digital transactions, Payment gateways, Online payments, Cyber security, Encryption, Blockchain technology.

I. INTRODUCTION

In India, a payment gateway serves as a vital component in the realm of online transactions. It acts as a secure link between customers and merchants, facilitating the smooth transfer of funds over the Internet [1]. Comparable to a traditional point-of-sale terminal, a payment gateway enables customers to make purchases using various electronic payment methods like credit cards, debit cards, online banking, and the Unified Payments Interface (UPI) [2]. Its primary role is to confirm the safety and integrity of transactions by encrypting sensitive financial data, verifying payment details, and protecting against fraud. This includes checking for sufficient funds, validating card information, and complying with strict regulatory standards set by the Reserve Bank of India (RBI) and other relevant authorities [3].

Payment gateways are indispensable for businesses operating in India's burgeoning digital economy, enabling them to accept payments seamlessly and securely. They cater to a wide range of industries, including retail, travel, hospitality, and entertainment, supporting both domestic and international transactions [4].

Compliance with industry standards like Payment Card Industry Data Security Standard (PCI DSS) is paramount to safeguarding sensitive information and building trust among consumers and merchants. As online shopping and digital payments continue to gain momentum, payment gateways play a crucial role in aiding the transition to a cashless economy, offering reliability, security, and convenience to all stakeholders involved [5].

A. Key Factor to choose Payment Gateway

Following are the main factors to choose the payment gateway:

- Compare transaction fees, including any hidden or additional charges.
- Assess the range of payment opportunities supported to satisfy the various customer preferences.
- Verify the currencies supported to accommodate international customers.
- Prioritize gateways with instant checkout options to streamline the payment process.
- Evaluate the payment settlement time to manage cash flow effectively.
- Prioritize security features like encryption and fraud detection to safeguard sensitive data.

II. BACKGROUND STUDY

The payment gateways in India work similarly to those in other countries but often have specific features tailored to the Indian market [6]. Here's a simplified explanation of how payment gateways function in India:

1) Customer Initiates Payment

The process starts when a consumer buys any product through an website or mobile app and chooses to pay using an online payment method such as credit/debit card, net banking, UPI (Unified Payments Interface), wallets (like Paytm, PhonePe, etc.), or other online payment system [7].

2) Encryption and Secure Transmission

Once the customer confirms the payment, the payment details (such as card information, UPI ID, etc.) are encrypted using SSL (Secure Socket Layer) technology to ensure secure transmission over the internet.

3) Forwarding to Payment Gateway

The encrypted payment information is then forwarded to the payment gateway selected by the merchant (the website or app where the purchase is being made). The payment gateway serves as an intermediary between the trader's website/app and the bank or monetary institution handling the transaction [8].

4) Authentication and Authorization

The payment gateway receives the payment information and performs various security checks, including verifying the authenticity of the transaction and checking for sufficient

2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON) | 979-8-3315-1859-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/DELCON64804.2024.10866177

funds in the case of card payments. If everything checks out, the payment gateway sends an authorization request to the customer's bank or card issuer.

5) Response from Bank

Once the authorization request is received, the customer's bank or card issuer reviews the transaction information and determines whether the consumer has enough money or credit limit to finish the transaction. After that, the bank replies to the payment gateway with an authorization response that states whether or not the transaction is accepted [9].

6) Transaction Authorization

If the transaction is permitted, the payment gateway notifies the merchant's website/app, and the customer's order is confirmed. The payment gateway also sends a confirmation to the customer, indicating that the transaction was successful.

7) Settlement

Following approval of the transaction, money is moved from the customer's bank or credit card company to the merchant's account via the payment gateway. Depending on the payment method and the terms of the merchant-payment gateway provider agreement, settlement periods may change.

8) Reporting and Reconciliation

Payment gateways typically provide merchants with tools for reporting and reconciling transactions, including transaction logs, settlement reports, and analytics to track sales and monitor payment activity.

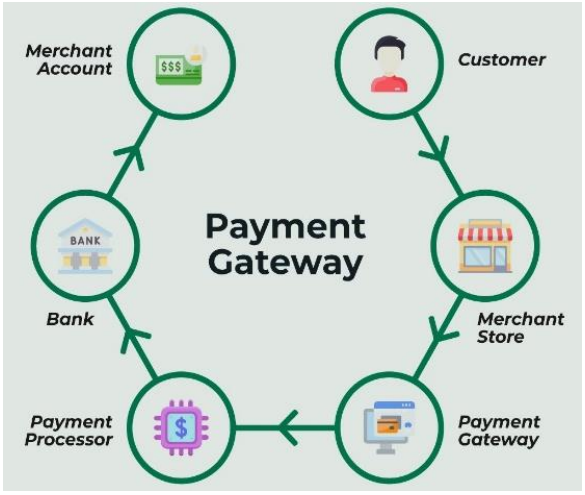

Fig. 1. Payment Gateway Process

In India, payment gateways also need to comply with regulations and standards set by regulatory bodies like the RBI and adhere to security standards such as PCI DSS to confirm the safety of online transactions. Additionally, they often integrate with popular Indian payment methods like UPI and digital wallets to cater to the preferences of Indian consumers [10]. Fig. 1 represents the overall payment gateway process of a digital transaction.

III. Different Case Studies

The landscape of online transaction gateways is diverse, with numerous providers catering to different regions, industries, and types of transactions [11]. Here are ten prominent online transaction gateways globally, covering a range of functionalities and market presence:

1) PayPal

One of the popular online payment gateways globally, offering services for individuals, businesses, and online sellers. Different payment mechanisms, like credit/debit cards, bank transfers, and PayPal balances are supported by PayPal [12].

2) Strip

A popular payment gateway for online businesses, providing APIs and tools to accept payments securely and seamlessly. Stripe is appropriate for companies that conduct business globally since it offers a broad choice of payment options and currencies.

3) Square

Recognized for its POS systems, Square also provides e-commerce companies with online payment processing solutions. Businesses may take payments through in-person transactions, mobile apps, and websites thanks to Square's platform.

4) Amazon Pay

Integrated with Amazon's ecosystem, customers can use their Amazon accounts to make purchases on websites run by third parties by using Amazon Pay. It offers a convenient checkout experience and supports various payment methods.

5) Apple Pay

With Apple's mobile payment service, customers may use their iPhones, iPads, and Apple Watches to safely make payments. Enhanced security features like Touch ID and Face ID identification are available with Apple Pay, which is widely recognized by retailers.

6) Google Pay

Google's online wallet and payment facility enable users to make online payments, in-app purchases, and peer-to-peer transactions. Google Pay integrates with various Google services and supports multiple payment methods [13].

7) Braintree

Owned by PayPal, Braintree offers payment handling mechanisms for industries of all sizes, offering features like seamless integration, recurring billing, and support for multiple currencies. Braintree is popular among startups and growing businesses.

8) Authorize.Net

A leading payment gateway provider in the United States, Authorize.Net offers solutions for accepting credit card and e-check payments online. It provides robust security features and customizable payment options for merchants.

9) Adyen

A global payment company that offers omnichannel payment solutions for businesses across various industries. Adyen supports a wide range of payment methods, currencies, and regions, making it suitable for international businesses.

10) Worldpay

A major player in the payment processing industry, Worldpay provides online payment solutions for e-commerce businesses, including secure payment processing, fraud prevention tools, and customizable checkout options.

These are just a few examples of prominent online

transaction gateways, and there are many other providers serving specific markets and industries with tailored solutions and features [14]]. Businesses should think about things like transaction costs, security features, and system compatibility when selecting a payment gateway. and support for desired payment methods and currencies.

IV. Analysis of Secure Online Money Transaction

Following are the current steps that are followed to secure online money transactions in India:

1) Encryption

Putting in place robust encryption mechanisms, like Secure Socket Layer (SSL) or Transport Layer Security (TLS), to safeguard private payment information when it is being transmitted between the customer's device, the business, and the payment gateway [15].

2) Two-Factor Authentication (2FA)

Employing additional authentication measures beyond passwords, such as SMS-based verification codes, biometric authentication, or token-based authentication, to validate the individuality of users and avoid illegal access to accounts [16].

3) Tokenization

Utilizing tokenization techniques to substitute sophisticated payment information, like credit card numbers or bank account credentials, with distinctive tokens that are meaningless to attackers, reducing the risk of data theft [17].

4) Compliance with Standards

Adhering to industry standards and regulatory requirements, such as PCI DSS, to confirm the implementation of robust security controls and practices for handling payment data securely.

5) Fraud Detection and Prevention

utilizing machine learning algorithms and sophisticated fraud detection systems to examine transaction patterns, identify questionable activity, and prevent fraudulent transactions in real-time.

6) Protected Payment Gateway

Select a reputable and secure payment gateway supplier that implements stringent security measures, undergoes regular security audits, and complies with regulatory standards to safeguard online transactions [18].

V. Results and Discussion

Here are some recommended guidelines that can be followed for secure online money transactions:

1) Improved Biometric Authentication

Integrating biometric verification technologies, such as facial recognition, fingerprint scanning, or voice acknowledgment, to provide stronger and more convenient authentication methods that are resistant to cyber threats like phishing and credential theft [19].

2) Blockchain Technology

Leveraging blockchain technique for a protected and translucent payment process, enabling decentralized and immutable ledger systems that enhance the security, transparency, and traceability of online payments while reducing the risk of fraud and data manipulation [20].

3) AI-Powered Cybersecurity

Utilizing artificial intelligence (AI) and machine learning (ML) algorithms to continuously investigate huge data, recognize emerging cyber threats, and proactively adapt security measures to mitigate risks and protect against evolving attack vectors [7].

4) Quantum-Safe Cryptography

Developing and implementing quantum-resistant cryptographic algorithms and encryption techniques to safeguard online transactions against potential threats posed by quantum computers, which could potentially compromise current encryption standards in the future [21].

5) Secure IoT Payments

Strengthening security measures for Internet of Things (IoT) devices used for making online payments, such as smart watches or connected appliances, to prevent vulnerabilities and unauthorized access that could be exploited by cybercriminals.

6) Collaboration and Information Sharing

Promoting cooperation between industry participants to exchange threat intelligence, best practices, and security insights in order to increase the resilience of the digital payment ecosystem against cyber-attacks. These stakeholders include payment processors, financial institutions, merchants, and cyber security experts [22].

A. Regulatory Compliance and Data Safety

Regulatory compliance and data safety are fundamental aspects of securing online money transactions, especially in the context of India's digital transaction landscape. As the digital economy expands and evolves, it becomes increasingly important for businesses and payment gateway providers to adhere to relevant regulations and standards while safeguarding sensitive customer information [23].

1) Compliance with Regulatory Standards

In India, the RBI and other regulatory bodies impose stringent regulations on financial transactions and data handling. Payment gateway providers essentially comply with these guidelines to confirm the legality and safety of their operations. This includes adhering to guidelines set forth by the RBI regarding online payment processing, data security, and fraud prevention. Failure to comply with regulatory standards can result in penalties, legal liabilities, and damage to reputation [24].

2) Data Protection Laws

Alongside regulatory standards, businesses operating in India must also comply with data protection laws to safeguard customer information. The Personal Data Protection Bill, when enacted into law, will introduce comprehensive data protection regulations, imposing obligations on businesses to collect, process, and store personal data responsibly. Payment gateway providers certainly apply robust data protection mechanisms to avoid unlawful access, data breaches, and misuse of customer data. This includes encryption of sensitive information, regular security assessments, and data access controls [25].

3) GDPR Compliance (if applicable)

For businesses operating internationally or catering to customers in the European Union (EU), compliance with the General Data Protection Regulation (GDPR) is essential. GDPR imposes strict requirements on the processing and

protection of EU residents' personal data, regardless of the business's location.

4) Risk Assessment and Mitigation

Regulatory compliance and data protection efforts should be accompanied by comprehensive risk assessment and mitigation strategies. This includes evaluating internal processes, third-party dependencies, and emerging cyber threats. Based on the risk assessment findings, appropriate mitigation measures should be implemented to address identified risks effectively [26].

5) Continuous Monitoring and Compliance Updates

The regulatory landscape and data protection requirements are subject to change, necessitating continuous monitoring and updates to compliance practices. Payment gateway providers must stay abreast of regulatory developments, industry standards, and best practices to adapt their compliance programs accordingly. This includes participating in industry forums, engaging with regulatory authorities, and investing in ongoing training and education for staff members [27].

6) Transparency and Accountability

Transparency and accountability are essential principles in regulatory compliance and data protection. Payment gateway providers should maintain transparency in their operations, policies, and data-handling practices to build trust with customers and regulatory authorities. Additionally, they should establish mechanisms for accountability, such as internal audit processes, compliance reporting, and incident response procedures, to ensure accountability for regulatory compliance failures and data breaches [28].

B. Continuous Security Monitoring and Incidence Response

Continuous security monitoring and incident response are crucial components of a robust cybersecurity strategy for payment gateway providers operating in India's digital transaction landscape. These measures involve proactive monitoring of systems and networks to identify and reply to safety incidents punctually, diminishing the effect of possible breaches and ensuring the ongoing security of online money transactions [29]. Fig. 2 shows the overall security development steps of digital transactions in India.

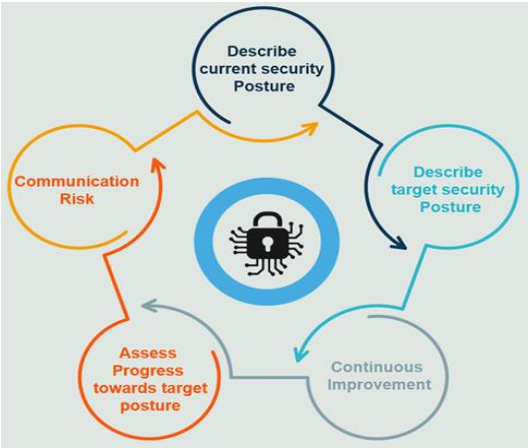

Fig. 2. Overall Security Development Steps of Digital Transaction

1) Continuous Threat Monitoring

Payment gateway providers should implement automated security monitoring tools and systems to continuously monitor their networks, applications, and infrastructure for potential security threats and vulnerabilities. This includes intrusion detection systems (IDS), security information and event management (SIEM) solutions, and threat intelligence feeds that help identify suspicious activities, abnormal behavior, and emerging cyber threats in real-time [30].

2) Incident Detection and Analysis

Upon detecting a security incident or anomaly, payment gateway providers must swiftly investigate and analyze the event to determine its nature, scope, and impact. This involves triaging alerts, conducting forensic analysis, and collaborating with internal security teams and external cyber security experts to assess the severity of the incident and formulate an effective response strategy.

3) Incident Response Planning

Payment gateway providers should develop comprehensive incident response plans that outline predefined procedures and protocols for responding to security incidents effectively. These plans should define roles and responsibilities, escalation procedures, communication protocols, and mitigation strategies to facilitate a coordinated and timely response to security breaches, data breaches, or other cyber incidents [31].

4) Mitigation and Remediation

Payment gateway providers are required to respond promptly to security incidents in order to minimize the damage and limit the problem. This may involve isolating affected systems, implementing temporary security controls, applying patches or updates to address vulnerabilities, and deploying countermeasures to prevent further exploitation of security weaknesses.

5) Communication and Notification

Transparent communication is essential during a security incident to keep stakeholders informed about the situation, its potential impact, and the steps being taken to address it. Payment gateway providers should establish communication channels and protocols for notifying customers, partners, regulatory authorities, and other relevant stakeholders about security incidents, ensuring transparency and maintaining trust in the integrity of their services [32].

6) Post-Incident Analysis and Remediation

Following the resolution of a security incident, payment gateway providers should conduct a thorough post-incident analysis to identify root causes, lessons learned, and opportunities for improving security posture. This involves conducting post-mortem reviews, updating incident response procedures based on lessons learned, and implementing corrective actions to prevent similar incidents from occurring in the future [33].

7) Continuous Improvement

Security is an ongoing process, and payment gateway providers should continuously evaluate and enhance their security posture based on emerging threats, evolving technologies, and lessons learned from past incidents [34]. This includes investing in cybersecurity awareness training for staff, conducting regular security assessments and penetration testing, and staying abreast of industry best practices and emerging security trends to adapt and strengthen their defenses against cyber threats.

By prioritizing continuous security monitoring and incident response capabilities, in order to protect online

financial transactions and preserve the faith and confidence of clients and stakeholders in India's digital transaction ecosystem, payment gateway providers can effectively detect, respond to, and mitigate security issues [35].

As India's digital transaction landscape continues to evolve, it is imperative for payment gateway providers to remain vigilant, adaptable, and committed to upholding the highest standards of security, compliance, and customer satisfaction. By staying ahead of emerging threats, embracing innovative solutions, and prioritizing the needs of businesses and consumers alike, payment gateway providers can play a pivotal role in shaping the future of digital payments in India and beyond [36]. In essence, the journey towards a secure and seamless digital transaction ecosystem requires continuous collaboration, innovation, and vigilance. As we navigate the challenges and opportunities ahead, let us remain steadfast in our commitment to driving positive change, fostering trust, and unlocking the full potential of India's digital economy.

VI. Conclusion

In conclusion, navigating India's digital transaction landscape requires a multifaceted approach that addresses the complexities of online payments while prioritizing security, compliance, and innovation. Payment gateway providers play a pivotal role in facilitating seamless and secure transactions between customers and merchants, enabling businesses to thrive in the rapidly evolving digital economy. Throughout this journal, we have explored the fundamental workings of payment gateways, highlighted key considerations for selecting a suitable payment gateway provider, and outlined essential steps to secure online money transactions effectively. From encryption and two-factor authentication to fraud detection and compliance with regulatory standards, payment gateway providers must implement robust security measures to safeguard sensitive financial data and build trust among consumers and merchants.

Looking ahead, the future of online payments in India holds immense promise, driven by advancements in biometric authentication, blockchain technology, artificial intelligence, quantum-safe cryptography, and secures IoT payments. By embracing these technologies and fostering collaboration among industry stakeholders, payment gateway providers can mitigate cyber threats, enhance transaction security, and propel India towards a cashless economy built on trust, reliability, and convenience.

References

[1] M. Sinha, H.Majra, J.Hutchins, and R. Saxena, “Mobile payments in India: the privacy factor”, International Journal of Bank Marketing, 37(1), pp.192-209, 2019.

[2] S. Chatterjee., R. Chaudhuri, D. Vrontis, and Z. Hussain., “Usage of smartphone for financial transactions: from the consumer privacy perspective.” Journal of Consumer Marketing, 40(2), pp.193-208. 2023.

[3] N.Pardhey, and D.N.Yuni, “Legal Efficiency of Secure Transactions Framework in India: A Multi-Dimensional Regulatory System”, In Fintech Applications in Islamic Finance: AI, Machine Learning, and Blockchain Techniques (pp. 171-182). IGI Global., 2024.

[4] V. Kandpal, “Dimensions of financial inclusion in India: a qualitative analysis of bankers perspective”, Qualitative Research in Financial Markets, 16(4), pp.660-679, 2024.

[5] A. Kesharwani, and S. S. Bisht, “The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model” International journal of bank marketing, 30(4), pp.303-322, 2012.

[6] R. K. Mishra and J. Kiranmai, “E-BANKING: A CASE OF INDIA” ICFAI Journal of Public Administration, 5(1).2009.

[7] D. Kumar and N. Goyal, “Security issues in M-commerce for online transaction”, 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 409-414). IEEE.2016.

[8] R. Thakur and M. Srivastava, “Customer usage intention of mobile commerce in India: an empirical study”,. Journal of Indian Business Research, 5(1), pp.52-72, 2013.

[9] S.Yuvaraj and N. S. Eveline, “Consumers’ perception towards cashless transactions and information security in the digital economy” International Journal of Mechanical Engineering and Technology, 9(7), pp.89-96, 2018.

[10] A. Kumar, “A study of significant characteristics of e-payment regime in India”. MERC Global's International Journal of Management, 7, pp.168-174, 2019.

[11] P. K. Kushwaha,V. Bibhu, B. P. Lohani, and D. Singh, “Review on information security, laws and ethical issues with online financial system”. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 49-53). IEEE, 2016.

[12] P. Kansal, “Online privacy concerns and consumer reactions: Insights for future strategies”. Journal of Indian Business Research, 6(3), pp.190-212, 2014.

[13] A.Khare, A. Mishra, and A. B. Singh, “Indian customers’ attitude towards trust and convenience dimensions of internet banking”. International Journal of Services and Operations Management, 11(1), pp.107-122, 2012.

[14] A. Khare and S. Singh, “Role of consumer personality in determining preference for online banking in India”. Journal of Database Marketing & Customer Strategy Management, 17, pp.174-187, 2010.

[15] N. P. Rana, , S. Luthra, and H. R. Rao, “Key challenges to digital financial services in emerging economies: the Indian context”. Information Technology & People, 33(1), pp.198-229, 2020.

[16] V. Bibhu, A. Kumar, B. P.Lohani, and P. K. Kushwaha, “Robust Secured Framework for Online Business Transactions over Public Network” In 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 555-560). IEEE, 2021.

[17] S. Nair, ,S. K. Khatri, and H. Gupta,, “A model to enhance security of digital transaction” 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 17-21). IEEE, 2019.

[18] K. K. Prasad, and P. Ushadevi, “An Online Comparative Study on Mobile banking Financial Transaction of Major Nationalized Banks in India”. Exploring Avenues In Banking, Management, It, Education & Social Sciences, p.209, 2018.

[19] S. A. Aljawarneh, “Online banking security measures and data protection. IGI Global, 2016.”

[20] G. Soana, de Arruda, T. “Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture” J Bank Regul, https://doi.org/10.1057/s41261-024-00241-2, 2024.

[21] E. Onyekwere, F. N. Ogwueleka, and M. E. Irhebhude, “Adoption and sustainability of bitcoin and the blockchain technology in Nigeria” Int. j. inf. tecnol. 15, 2793–2804, , 2023.

[22] D. Singhal, L. Ahuja, and A. Seth, “POSMETER: proof-of-stake blockchain for enhanced smart meter data security” Int. j. inf. tecnol. 16, 1171–1184, 2024.

[23] C. S. Tiwari, V. K. Jha, “THC-DFECC-based privacy preserved smart contract creation for cloud data security”. Int. j. inf. Tecnol, https://doi.org/10.1007/s41870-024-02040-4, 2024.

[24] S. Singh, and R. K. Srivastava., “Predicting the intention to use mobile banking in India”. International Journal of Bank Marketing, 36(2), pp.357-378, 2018.

[25] P. V. Ranjith, S. Kulkarni, and A. J. Varma, “A literature study of consumer perception towards digital payment mode in India” Psychology and Education, 58(1), pp.3304-3319, 2021.

[26] C. P. Chandrasekhar and J. Ghosh,, “The financialization of finance? Demonetization and the dubious push to cashlessness in India”. Development and change, 49(2), pp.420-436, 2018.

[27] V. Khattri, and D. K. Singh, “Implementation of an additional factor for secure authentication in online transactions”. Journal of Organizational Computing and Electronic Commerce, 29(4), pp.258-273, 2019.

[28] M. K. Normalini and T. Ramayah, “Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of

biometrics technology on perceived privacy and security". Journal of Management Sciences, 4(1), pp.3-26, 2017.

[29] P. Datta, S. N. Panda, S. Tanwar, and R. K. Kaushal,. "A technical review report on cyber-crimes in India". International conference on emerging smart computing and informatics (ESCI) (pp. 269-275). IEEE, 2020.

[30] K. K. Gupta,. and I. Bansal, "Development of an instrument to measure internet banking service quality in India". Researchers World, 3(2 Part 2), p.11, 2012.

[31] R. Kumar, S. Kishore, H. Lu, and A. Prakash, "Security analysis of unified payments interface and payment apps in India". In 29th usenix security symposium (usenix security 20) (pp. 1499-1516), 2020.

[32] A. Mashatan, M. S. Sangari, and M. Dehghani, "How perceptions of information privacy and security impact consumer trust in crypto-payment: an empirical study". IEEE Access, 10, pp.69441-69454, 2022.

[33] R. Sarkar and S. Das, "Digitalization and its impact on financial transactions in India," Frontiers of Digital Finance, 2018.

[34] A. Mahalle, J. Yong, X. Tao, and J. Shen, "Data privacy and system security for banking and financial services industry based on cloud computing infrastructure," In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 407-413). IEEE, 2018.

[35] S. Sudeep and K. C. Sankaranarayanan, "Internet banking and customer acceptance: the Indian scenario", Doctoral Dissertation, Cochin University of Science & Technology, 2008.

[36] A. Pal, T. Herath, and H. R. Rao, "Why do people use mobile payment technologies and why would they continue? An examination and implications from India". Research Policy, vol. 50, no.6, pp.104228, 2021.