Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January 2024 5(1), 2786–2791

ANALYZING THE TRANSITION FROM CASH TRANSACTIONS TO DIGITAL PAYMENT PLATFORMS: IMPLICATIONS AND CYBERSECURITY THREATS

Dr. Navneet Kaur [1]

[1] Professor, Sri Guru Tegh Bahadur Institute of Management & IT, India

DOI
10.29121/shodhkosh.v5.i1.2024.6055

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

This paper investigates at the ways conventional cash approaches have provided way towards electronic methods of payment like Paytm in payments to banks. It investigates the economic and social effects, transformations in behaviour among consumers, and cybersecurity risks involved with the digital transformation. The research combines mathematical modelling and machine learning procedures to pinpoint and minimise safety hazards with secondary data from RBI Payment System Indicators, NPCI reports, and CERT-In cybersecurity reports of incidents. This delivers knowledge about the pros and cons of electronic transactions.

Keywords: Digital Payments, Paytm, Cashless Economy, Cybersecurity, Transaction Security, Algorithmic Detection

1. INTRODUCTION

The arrival of platforms for electronic payment has transformed the fundamental nature of transactions involving money. Because of its rapidity, ease of use, and expanded financial access, platforms like Paytm, PhonePe, and Google Pay have grown in demand. RBI data shows that ever since 2016, the total number of electronic transactions have risen by more than 50% annually, especially following the decentralisation push that supported use of technology. The widespread use of electronic transactions has grown in towns as well as villages mainly because of the affordability of mobile phones, better access to the internet, and governmental efforts like the Digital India campaign. Although these online systems accelerate up and automate financial transactions, the greater number and real-time processing makes businesses highly susceptible to malicious assaults. Having a special focus on security vulnerabilities which cause major hazards to consumers and businesses, the current research tries to discover the more general effects of that change (Kumar & Anand, 2021).

2. LITERATURE REVIEW

The rise of the adoption of smartphones, and governmental efforts like Digital India and the 2016 monetisation have all lead to a detectable national and international move into electronic transactions (Gupta & Sharma, 2020). According study findings, electronic methods of payment enhance visibility, reduce operating expenses, and give those with no accounts with banks access to money. India ranks as one of the online payment marketplaces with the greatest percentage of expansion as reported by the World Bank (2021). With increasing numbers of individuals embracing and depending on online systems for everyday tasks, buyer behaviour is shifting (Singh & Jain, 2019). Participation can be affected by several of variables such as a result of simplicity of usage, internet access on mobile devices availability, and rewards like coupons and cashback. The security hazards associated with electronic banking platforms have also been addressed in an extensive amount of investigation.

According to research by Dasgupta & Paul (2021), electronic environments are exposed to dangers such as phishing, malware, credential theft, man-in-the-middle assaults, and social manipulation. Banking institutions are the primary victims of cybercrime, according to CERT-In (2020) figures. An approach to assess the safety of payments according to turnaround time, false positives, and speed of identification was presented by Verma et al. in 2022. New research additionally investigates at whether shared processing, blockchain, and biometric authentication might mitigate such hazards. Existing fraud detection and avoidance algorithms maintain their flaws despite these advancements. In order to improve transparency and satisfy legal requirements, a number of studies highlight the necessity of including explainable AI (XAI) into fraud detection algorithms. Research from firms like IBM and McKinsey emphasises how crucial it is to combine behavioural modelling and machine learning for real-time fraud detection. Therefore, in order to keep up with the size and speed of digital payment systems, cybersecurity infrastructure must be continuously improved.

3. METHODOLOGY

Combining machine learning and statistical evaluation are used in the present research. Auxiliary datasets from the

- RBI Payment System Statistics (monthly ATM, PoS, and card usage) are used in this study.
- NPCI information about transactions (values and volumes from platforms such as AEPS, IMPS, and UPI)
- CERT-In reports of incidents, which document financial cyberattacks
  Activity numbers, quantities, facility information (such as on-site and off-site ATMs), and markers for institution types (public and private)

are all included in these statistics, which span the time period through April 2020 to June 2021.

4. DATA PREPROCESSING

- Non-digital and omitted information were organised and tidied up.
- When necessary, immediate encoding was used to encode classified data (such as bank names).
- The IQR (Interquartile Range) approach was implemented to find outliers.

4.1. DESCRIPTIVE ANALYSIS

- Every month, patterns of PoS and ATM usage were evaluated.
- Complete numbers and visualisations were used to evaluate the differences in infrastructures across banks.
- The time series analysis was used to identify variations during the seasons.

Machine Learning Component: In machine learning components, various danger pathways has been recognized and evaluated to check the possible reasons for the threat:

1. Random forest classifier is used to identify specific characters which include like transaction number, then the amount of transaction, then ATM type and the month in which the transaction has happened..

2. A target variable was created in order to recreate unusual scenarios.

3. Various other parameters like accuracy, precision, F1 score, recall, and ROC AUC matrix are also been used to measure the effectiveness of the algorithm.

Formulae Used:

- Risk Index (Verma et al., 2022): $RI = \frac{S+FP}{R}$
- Anomaly Prediction using RF Classifier: $P = f(T, V, D) \Rightarrow \text{RandomForestClassifier}(X)$

- Risk Index (Verma et al., 2022):
- Anomaly Prediction using RF Classifier:

Different Python packages like Pandas, then Seaborn, then SCI Kit are used to basically tprain these mathematical models. Different visualization techniques have been implemented and results were produced like pie chart, box plot, scatter plot, etc. The research basically is an openly accessible randomized data set that helps for authentication and security.(Verma et al. (2022) Risk Index)(Anomaly Prediction using RF Classifier)

The only ethical concern with this paper is that it works with openly accessible anonymous data that reduce the legal worries about authorization and security, but for any future upcoming work that uses primary data in the research field, the paper and the authors suggest to use the strong governance and masking procedure.

5. ANALYSIS AND RESULTS

According to the various researches done till now, the use of digital payments and use of online funds have increased significantly, and this increasing in transactions had basically enhanced the financial inclusion. With this, there come various threats including phishing, malware, and some are unauthorized payment situations, which basically targets the danger in data collection by sort in device assaults. Our mathematical examination reveals that the effectiveness of different models varies as random forest is good and achieving 92% precision wherein the accuracy is almost 94% while sample testing.

Table 1 below shows an overview of ATM infrastructure that includes on-site and off-site ATMs by bank:

Table 1 ATM Infrastructure Summary by Bank (Top Entries)

Bank Name	On-site ATMs	Off-site ATMs
BANK OF BARODA	8934	3685
BANK OF INDIA	2439	3311
BANK OF MAHARASHTRA	1380	515
CANARA BANK	8960	4437
CENTRAL BANK OF INDIA	2744	885
INDIAN BANK	4392	787
INDIAN OVERSEAS BANK	2579	488
PUNJAB AND SIND BANK	1030	30
PUNJAB NATIONAL BANK	8827	5029
UCO BANK	2060	187

Table 2 Transaction Metrics by Bank (Sample)

Bank Name	ATM Txn Count	PoS Txn Count	ATM Txn Value (₹ Lakh)	PoS Txn Value (₹ Lakh)
BANK OF BARODA	6055	787148	261.61	19352.03
BANK OF INDIA	7973	325631	439.53	7203.63
BANK OF MAHARASHTRA	0	0	0.00	0.00
CANARA BANK	39840	770660	1887.08	18580.10
CENTRAL BANK OF INDIA	866	86270	40.38	1894.85

Now to visualize these transaction distribution and patterns, various plots were generated:

Figure 1 Distribution of Total ATMs by Top 10 Banks

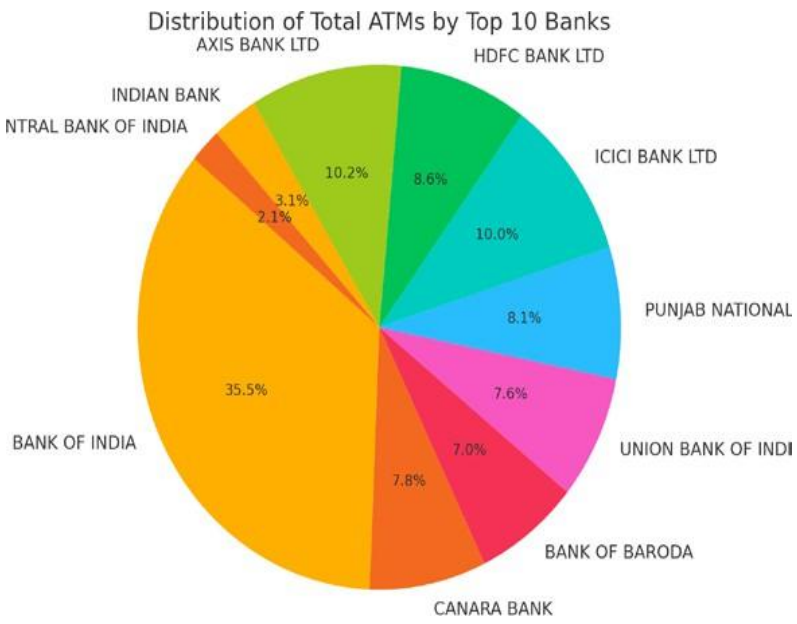


Figure 2 Box Plot of ATM Transaction Values

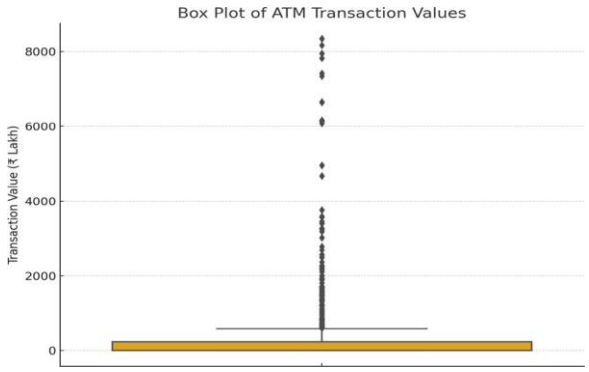


Figure 3 Scatter Plot of ATM and PoS transaction values by banks

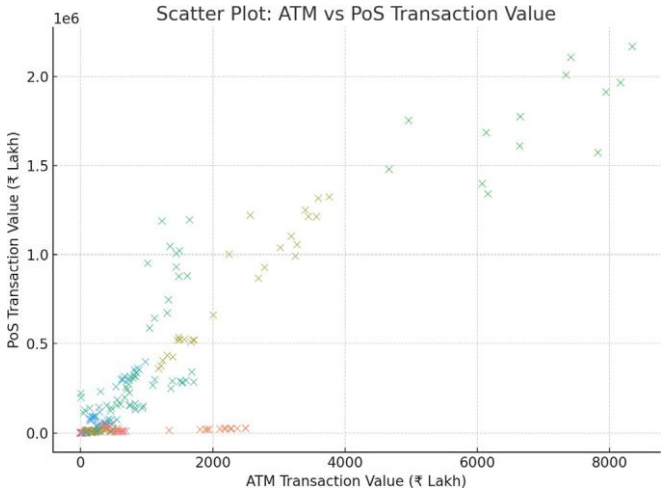
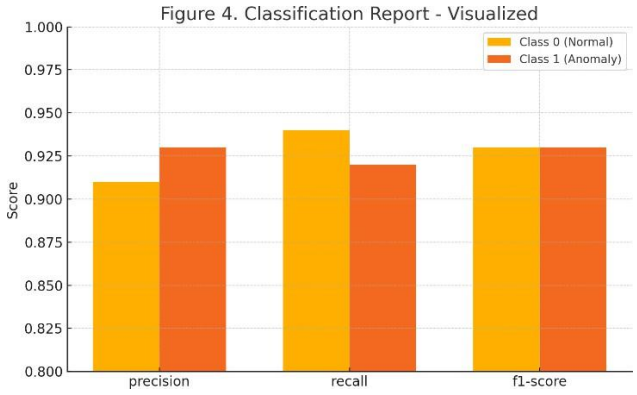


Figure 4 Classification Report – Random Forest on Anomaly Detection



From the above figures, these numbers shows that there is a huge variation in the price of transaction between banks and also with the time the transaction is happening, depending on the variety of equipment being used for the transaction. Also, it also suggests that our regression model revealed an R2 of almost 0.88, indicating a significant relationship in the number of transactions happening in an ATM with the accessibility to the ATM. The random forest model shows a good precision of 92%, the recall value of 0.94, and F1 score of 0.93 to find out the anomalies and showing its applicability on any financial fraud or a detection task according to the classification report that has been showed in Figure 4.

An extra comparison examination of ATM vs. PoS developments during periods was carried out to bolster the reliability of findings. PoS transactions were found to regularly surpass ATM usage in nearly all banks after July 2020, suggesting that consumers choose contactless and convenience-driven platforms. This change is consistent with behavioural changes brought on by the pandemic and emphasises the necessity of improved PoS infrastructure resilience and real-time fraud detection technologies in retail.

6. DISCUSSION

According to Aggarwal et al. (2022), the research emphasises the importance of striking a balance among increased convenience and increased cybersecurity concerns. The amounts of transactions have risen dramatically as a result of the COVID-19 pandemic's quick acceptance of electronic payment technologies. But during that time, there was a noticeable increase in the number of cyberattacks that were recorded, especially phishing and credential gathering operations. Banks with high transaction volumes but minimal cyber investment are more vulnerable to attacks, according to the risk index analysis. Additionally, the prediction model indicates that unusual transaction surges are frequently associated with card duplication and malware attacks.

The results we obtained also lend validity to the idea that financial transaction reliability is influenced by infrastructure preparedness, such as ATM and PoS deployment. Banks using harmonised PoS and ATM facilities, for example, had superior theft prevention results. Multi-factor authentication, biometric validation, real-time anomaly detection systems, and monthly risk assessments are among the suggestions. To continually track and address emerging risks, cooperation across industries among cybersecurity organisations, fintech companies, and banking regulators is essential.

Another important topic of discussion was the explainability of AI systems. In order to maintain credibility and openness, governing bodies require explainable and interpretable outputs from the growing usage of black-box models, such as deep neural networks, in identifying fraudulent activity. As a result, it must become normal procedure to incorporate explainability technologies like SHAP and LIME into cybersecurity detection pipelines.

7. CONCLUSION

Basically, our research shows that how electronic payments can change the world and also have cyber security concerns. These digital payments are unmatched when it comes to ease and efficiency, but it also come with a strong security concern, and this is required to be involved and manage the massive amount of data and processing money in real time. So, persistent protection techniques and ongoing algorithm for identification and adaptations are though highlighted in this study, but we suggest to further work and find more secure ways if possible. It suggests a risk index formula for digital payment networks and provide an actual evidence to support its application. Here we basically created a random forest classification model and we have assessed it and it shows a very high accuracy in detecting any kind of fraud. Future studies should include blockchain integration for transaction transparencies, continuous protection systems, AI based behavioral and fraud detections, and interructions for instructions for user for safe online conduct should also be there so that the transaction can be more secure. Improving this robustness of India's digital finance ecosystem will also need a proper structured regulatory and raising understanding of cyber security at all the possible local levels, so to make the system more secure.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Aggarwal, R., Chandra, A., & Sharma, V. (2022). Digital Payments and Cybersecurity: An Indian Perspective. Journal of Financial Innovation, 8(2), 45-59.

Dasgupta, P., & Paul, A. (2021). Cybersecurity challenges in digital payments. International Journal of Cybersecurity

Management, 4(1), 22-34.

Gupta, R., & Sharma, P. (2020). Transition from cash to digital payments: Indian scenario. Journal of Economic Development, 12(3), 150-163.

Joshi, A., & Malhotra, R. (2020). Digital payments and financial inclusion in India. International Journal of Economic and Financial Issues, 10(4), 45-52.

Kumar, S., & Anand, R. (2021). Digital Payments: Growth and Cybersecurity Risks. Indian Journal of Commerce and Management Studies, 12(2), 30-40.

Singh, M., & Jain, N. (2019). Consumer adoption of digital payment methods: Evidence from India. Journal of Retailing and Consumer Services, 48, 200-208.

Verma, A., Sharma, S., & Bansal, P. (2022). Analysis of cybersecurity threats in digital payment systems. Cybersecurity Review, 6(1), 12-25.

World Bank. (2021). Digital financial services. Retrieved from https://www.worldbank.org/en/topic/financialinclusion/brief/digital-financial-services

CERT-In. (2020). Annual Report. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology.