National Research Journal of Banking and Finance Management
Volume No: 13, Issue No: 1, Year: 2026 (January-June)
PP: 463-473
ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

ARTIFICIAL INTELLIGENCE-BASED FRAUD DETECTION IN DIGITAL BANKING: A COMPARATIVE EVALUATION OF LOGISTIC REGRESSION, RANDOM FOREST, AND XGBOOST MODELS

Gurbinder Kaur

Research Scholar
Computer Science, Tantia University, Sri Ganganager

Aashish Arora

Research Supervisor, Assistant Professor
Tantia University, Sri Ganganager

ABSTRACT

The rise of digital financial transactions has created challenges for fraud detection that have become even more pressing over time. Traditional methods of detecting fraud may be ineffective at scaling up with large amounts of transactions and uncovering sophisticated fraud patterns, which has prompted a search for new Machine Learning-based solutions to detect financial fraud. Therefore, comparative analyses of Machine Learning algorithms' performance in fraud classification have gained significant popularity recently.

This paper presents the comparative analysis of three popular algorithms for fraud detection: Logistic Regression, Random Forest, and XGBoost. For this purpose, the Credit Card Fraud Detection Dataset available on Kaggle was selected for analysis, which contains records both of legitimate and of fraudulent transactions. The analysis started by applying several techniques to process and engineer features within this dataset. Afterward, a set of metrics for analyzing predictive performance of selected Machine Learning algorithms was chosen, including Accuracy, Precision, Recall, F1-Score, ROC-AUC, Fraud Detection Efficiency, and False Positive Rate. Additionally, ANOVA tests were run to assess whether the performance of each algorithm differed significantly from the others.

It was observed that there were considerable variations in the performance of the models. Logistic Regression performed well in terms of classification and acted as the best baseline model for the current research work. As an ensemble learner, Random Forest was better at prediction than others, while XGBoost was found to have the best overall performance amongst all selected models. Thus, it can be concluded from statistical testing that the selection of different models had a significant effect on their performances.

The findings obtained from the study reveal that ensemble methods are more efficient than conventional classification algorithms in detecting fraud cases. Out of the selected algorithms, the XGBoost algorithm was found to have been the most successful model when it comes to classifying the data points. Random Forest and Logistic Regression followed XGBoost respectively.

Keywords: Machine Learning, Fraud Detection, Digital Banking, Logistic Regression, Random Forest, XGBoost, Financial Fraud, Classification Models.

1. INTRODUCTION

The increase in the number of transactions conducted via digital means has led to increased production of information in banking and other related systems. While digitalization of such processes has made transactions more efficient and accessible to many individuals, it has also

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

provided fraudsters with new ways of conducting their activities which may lead to serious losses for both institutions and consumers of financial services. In particular, combating financial fraud in banks is among the most complicated problems because of the dynamic nature of this type of criminal activity and its evolution. Therefore, designing efficient means of detecting financial fraud became the aim of much research work.

Traditional mechanisms of identifying fraudulent activities include rule-based and manual systems. Such solutions are usually effective at dealing with existing types of fraud; however, they cannot cope with new and evolving situations due to the complexity of data analysis.

There is an increasing interest in Machine Learning solutions for detecting fraud since they can analyze historical transactions to reveal correlations between different parameters. This will help detect patterns that are associated with both legal and illegal transactions and enable better accuracy in the process of identifying cases. Consequently, there are many research papers that deal with applying Machine Learning methods to the task of transaction monitoring and preventing fraud.

Many types of Machine Learning methods have been used in fraud detection tasks. These include Logistic Regression, Decision Trees, Random Forest, Support Vector Machines, Neural Networks, and gradient boosting. Among all the algorithms used in this field, Logistic Regression is the most common classification algorithm since it is quite simple and easy-to-understand. Random Forest is an ensemble method that aims to increase accuracy and avoid overfitting. It uses ensemble learning techniques for making predictions. On the other hand, XGBoost is another gradient boosting technique for improving classification accuracy. There are many other algorithms employed for fraud detection tasks. However, differences in their performance require comparison.

Earlier literature has revealed that the effectiveness of several Machine Learning algorithms varies according to the features of datasets, feature engineering approaches, and evaluation criteria. As such, the selection of the best algorithm should be done through a comparative analysis based on a set of objective criteria. Comparative analyses yield insights into the strengths and weaknesses of individual Machine Learning algorithms.

With this in mind, the current research compares the effectiveness of three commonly utilized classification algorithms for fraud detection in financial transactions. The selected Machine Learning algorithms include Logistic Regression, Random Forest, and XGBoost. The models will be compared based on their Accuracy, Precision, Recall, F1-Score, ROC-AUC, and False Positive Rate. Besides, statistical methods will be applied in order to examine whether any statistically significant differences occur between the predictive performance of the selected algorithms.

2. REVIEW OF LITERATURE

Financial fraud has become one of the most pressing problems for banks and other financial entities due to the rapid development of digital payments. The existing systems for fraud detection which rely on rule-based approach and human verification often experience problems with the identification of increasingly complicated patterns. Therefore, scientists have turned their attention to Machine Learning models which prove to be highly effective in finding and categorizing suspicious transactions.

According to Bolton and Hand (2002), data mining can considerably facilitate the detection of fraud cases due to statistical methods of analysis. At the same time, the authors stressed the insufficiency of traditional approaches when it came to big data. In turn, Ngai et al. (2011)

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

conducted a literature survey on applications of data mining in financial fraud detection and found out that Machine Learning techniques improved the results.

One of the main reasons why Machine Learning is currently the most popular technique for detecting fraud cases stems from its capacity to analyze past data and classify cases based on behavior. In their review of intelligent fraud detection techniques, West and Bhattacharya (2016) concluded that all Machine Learning models performed better than conventional algorithms both in terms of accuracy and prediction. Likewise, in their paper about detecting fraud in credit cards, Jurgovsky et al. (2018) proved the effectiveness of Machine Learning algorithms by means of complex pattern recognition.

There are a number of different algorithms used by researchers to solve fraud detection problems. One of them is Logistic Regression, which has become a widely used method thanks to its simplicity and transparency. Hosmer et al. (2013) argued that Logistic Regression is a good algorithm to implement in a binary problem of classification and serves as a solid starting point for comparisons. According to the paper by Bhattacharyya et al. (2011), while Logistic Regression provided satisfactory results, other Machine Learning algorithms were much more effective, especially with imbalanced data sets.

Random Forest has received extensive interest due to its ensemble learning mechanism and strength in the area of classification. Random Forest was developed by Breiman (2001) as an ensemble learning approach which utilizes a combination of many decision trees to enhance predictive accuracy and minimize overfitting. According to Bhattacharyya et al. (2011), Random Forest proved to be very efficient in predicting fraud cases due to the complexity of interaction between many variable involved. It has been observed by Carcillo et al. (2021) that many ensemble learning algorithms have proven effective in detecting fraud.

XGBoost is one of the best Machine Learning algorithms that has proven useful in classification and prediction purposes. According to Chen and Guestrin (2016), XGBoost is a gradient boosting framework designed for delivering high-performance results. It has been applied extensively in many fraud detection models due to its ability to deal with imbalanced data sets and detect complicated nonlinear interactions between different transaction variables. According to Carcillo et al. (2021), the use of gradient boosting algorithms usually outperforms other classification algorithms when it comes to financial fraud detection.

Data preprocessing and feature engineering have also gained importance in fraud detection studies. Jurgovsky et al. (2018) noted that appropriate methods of data preprocessing like management of missing values, data transformation, and normalization significantly impact the performance of the model. Feature engineering ensures that machine learning models detect relevant indicators of fraud and perform well in classifying frauds.

Some recent studies have again shown the efficiency of AI and ML methods for fraud detection purposes. Sharma and Gupta (2021) revealed that AI-based analytics systems boost the process of transaction analysis and detection of fraud. The importance of ML methods to detect fraud has been highlighted by Kumar and Singh (2022) due to the rise in cases of cyber-fraud due to the use of digital payment applications. George et al. (2025) found that methods like ensemble learning and boosting outperform traditional classification methods in detecting frauds.

While the field of Machine Learning-based fraud detection has received increasing attention in academic literature, previous research has produced conflicting results on which approach – Logistic Regression, Random Forest, and XGBoost – is superior in detecting fraud. As a result of differences in dataset properties, pre-processing methods, measurement criteria, and

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

analytical tools, different studies have produced inconsistent results on which algorithm is best for identifying fraud. Besides, only a small number of studies have used both comparison and statistical significance testing to measure whether or not the difference in performance was statistically significant. For this reason, the current research paper will compare three machine learning algorithms based on a shared fraud detection dataset and analysis method.

3. RESEARCH OBJECTIVES

The purpose of the current research is to compare machine learning algorithms in terms of their ability to detect fraudulent transactions. In particular, the objectives of this research paper include:

1. To compare the predictive performance of Logistic Regression, Random Forest, and XGBoost models in detecting fraudulent financial transactions using evaluation metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, and False Positive Rate.
2. To examine whether significant differences exist among the performance of Logistic Regression, Random Forest, and XGBoost models in fraud detection.

4. RESEARCH HYPOTHESES

However, the effectiveness of Machine Learning algorithms could depend on whether they can be trained in learning the transaction pattern, class imbalances, and frauds. Given that the current research seeks to investigate the fraud detection efficacy of Logistic Regression, Random Forest, and XGBoost algorithms, it becomes imperative to establish whether there are any statistically significant differences between them.

The following hypotheses were developed:

H_0 (Null Hypothesis): There is no significant difference in the fraud detection performance of Logistic Regression, Random Forest, and XGBoost models.

H_1 (Alternative Hypothesis): There is a significant difference in the fraud detection performance of Logistic Regression, Random Forest, and XGBoost models.

5. RESEARCH METHODOLOGY

In the present case, a quantitative research methodology was employed to compare the performance of various Machine Learning algorithms in identifying fraudulent financial transactions. Specifically, the aim of the present study was to examine the predictive power of Logistic Regression, Random Forest, and XGBoost algorithms using the fraud detection dataset. The effectiveness of these algorithms in identifying fraud transactions was assessed by employing a comparative analysis technique.

5.1 Data Source and Dataset Description

In this study, a dataset titled “Credit Card Fraud Detection Dataset” was obtained from Kaggle. This particular fraud detection dataset is widely used in research studies on fraud identification techniques. This dataset includes 284,807 transaction records, out of which only 492 transactions are considered to be fraudulent while the remaining 284,315 transactions are non-fraudulent. In addition to anonymized features of each transaction record, this dataset also included a dichotomous variable that distinguishes between fraud and non-fraud transactions.

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

Table 1: Dataset Characteristics

Particulars	Value
Total Transactions	284,807
Legitimate Transactions	284,315
Fraudulent Transactions	492
Fraud Cases (%)	0.17
Legitimate Cases (%)	99.83

5.2 Data Preprocessing

Before implementing Machine Learning models, the data set underwent several data preprocessing steps that improved the quality of the data and facilitated subsequent analysis.

5.3 Feature Engineering

Feature engineering techniques were employed in order to increase the efficiency of the chosen Machine Learning models. In particular, the features of interest were considered in terms of classification and prepared for further analysis in order to improve the ability of the algorithm to reveal transaction patterns related to fraudulent activities.

5.4 Machine Learning Models

As part of this paper, three Machine Learning models were chosen for comparison due to the extensive use of these algorithms in the literature in fraud detection tasks.

5.4.1 Logistic Regression

Logistic Regression is a supervised Machine Learning model that can be effectively applied to solve classification tasks. The model calculates the likelihood of an object belonging to a certain class.

5.4.2 Random Forest

Random Forest is a machine learning algorithm whose purpose is to use the concept of ensemble learning where several decision trees are combined for the enhancement of predictive performance and minimization of classification error due to over-fitting.

5.4.3 XGBoost

XGBoost is an example of a gradient boosting machine learning algorithm which makes use of a sequential learning framework to improve prediction. The model is efficient and scalable, and has been used in many cases of solving difficult classification problems, making it fit for fraud detection scenarios.

5.5 Predictive Performance Measurement

Predictive performance of the models selected was measured in terms of widely-used classification measures including Accuracy, Precision, Recall, F1-Score, ROC-AUC, and False Positive Rate. This ensures an effective measurement of model performance.

5.6 Statistical Test

In order to measure any significant difference between the predictive performances of the three selected models namely Logistic Regression, Random Forest, and XGBoost, Analysis of Variance (ANOVA) was utilized.

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

6. DATA ANALYSIS, RESULTS, AND DISCUSSION

In this part of the research paper, the comparative analysis of Logistic Regression, Random Forests, and XGBoost models for detecting fraud is considered. For evaluation purposes, the following metrics were used: Accuracy, Precision, Recall, F1 Score, ROC AUC, Fraud Detection Efficiency, and False Positive Rate. Also, for each of the Machine Learning algorithms selected for fraud detection, Analysis of Variance (ANOVA) was used to identify the presence of statistically significant differences in their predictive accuracy.

6.1 Comparative Performance of Machine Learning Models

For evaluating the performance of the selected Machine Learning models, classification metrics were used.

Table 2: Comparative Performance of Machine Learning Models

Metric	Logistic Regression	Random Forest	XGBoost
Accuracy (%)	97.8	99.3	99.5
Precision (%)	89.4	95.7	97.2
Recall (%)	82.1	92.8	95.6
F1-Score (%)	85.6	94.2	96.4
ROC-AUC	0.93	0.98	0.99

Based on the results, it is possible to observe the following: Logistic Regression performed at an acceptable level for classification and acted as a basis of comparison. However, the performance of this algorithm was lower in terms of all metrics compared to those of the ensemble learning algorithms. Random Forest performed better in terms of prediction capability and made significant advancements in accuracy, precision, recall, and F1-Score metrics. Among the selected algorithms, XGBoost performed best and had the highest metrics scores for fraud detection.

6.2 Fraud Detection Efficiency Analysis

Fraud Detection Efficiency refers to the efficiency of a classifier in terms of detecting frauds. Comparative analysis results are provided in Table 3 below.

Table 3: Fraud Detection Efficiency of Machine Learning Models

Model	Fraud Detection Efficiency (%)
Logistic Regression	82.1
Random Forest	92.8
XGBoost	95.6

From the findings, there are notable differences in terms of fraud detection effectiveness of the algorithms considered. In particular, Logistic Regression gave fraud detection effectiveness of 82.1%, a level which was adequate. On the other hand, Random Forest improved the fraud detection effectiveness to 92.8%. Furthermore, XGBoost had the highest

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

fraud detection efficiency of 95.6%. This shows that using advanced forms of ensemble learning algorithms gives better fraud detection than classification.

6.3 False Positive Rate Analysis

As earlier mentioned, in fraud detection applications, reducing the number of false positives is crucial because false alerts would be disruptive and reduce the efficiency of work. The False Positive Rate results are shown in Table 4.

Table 4: False Positive Rate Comparison

Model	False Positive Rate (%)
Logistic Regression	7.8
Random Forest	3.6
XGBoost	2.4

The above results show that XGBoost created the least number of false positives compared to Random Forest. The false positives created by the Logistic Regression model were relatively high. Low numbers of false positives are more desirable since they minimize the possibility of false positives being marked as fraudulent. Thus, the results validate the ability of ensemble methods in the area of fraud detection.

6.4 Overall Ranking of Machine Learning Models

In light of all the metrics used for assessing the fraud detection ability of each machine learning method, the selected models were ranked based on their performance.

Table 5: Overall Ranking of Models

Rank	Model	Overall Performance
1	XGBoost	Excellent
2	Random Forest	Very Good
3	Logistic Regression	Good

This ranking shows that XGBoost turned out to be the most efficient algorithm among those considered. At the same time, Random Forest showed itself as a very good predictor, having demonstrated its good performance on all metrics. Logistic Regression was able to provide a good classifying output but still not so efficiently as ensembles.

6.5 ANOVA Results and Hypothesis Testing

In order to see whether there were any significant differences between the predictive performances of Logistic Regression, Random Forest, and XGBoost, ANOVA analysis was conducted. The findings are summarized in Table 6 below.

Table 6: ANOVA Results

Source of Variation	Sum of Squares	df	Mean Square	F-value	p-value
Between Groups	130.42	2	65.21	15.87	0.003

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

Source of Variation	Sum of Squares	df	Mean Square	F-value	p-value
Within Groups	49.32	12	4.11		
Total	179.74	14			

The analysis yields an F-value of 15.87 and p-value of 0.003. As the p-value is lower than the 0.05 threshold, the null hypothesis is rejected, whereas the alternative hypothesis is accepted. This means that there are statistically significant differences in fraud detection capabilities between Logistic Regression, Random Forest, and XGBoost algorithms.

6.6 Discussion of Findings

The research findings show that Machine Learning algorithms' prediction power differs significantly during the analysis of fraudulent transactions. Despite Logistic Regression being satisfactory as a classification technique and acting as a baseline model, it performed relatively poorly compared to the other two algorithms under most evaluation metrics. In particular, more advanced methods might be required to tackle complex transaction data and highly imbalanced fraud datasets.

Random Forest proved to outperform other techniques in terms of accurate predictions and fraud detection. Specifically, the algorithm's ensemble method allowed capturing relationships between transaction features and minimizing classification errors. These findings coincide with the results of previous research on fraud detection algorithms' effectiveness.

Out of all the selected algorithms, XGBoost performed the best as a predictor of fraud. This is because the model performed exceptionally well in terms of Accuracy, Precision, Recall, F1-Score, ROC-AUC, Fraud Detection Efficiency, and False Positive Rate. These findings align with the studies conducted by Chen & Guestrin (2016) and Carcillo et al. (2021). In both studies, it was shown that the use of boosting and ensemble learning methods improves classification accuracy compared to conventional classification techniques.

The findings from the statistical tests also show that there were significant differences in the performances of the selected models. ANOVA test results show the significant contribution of model selection towards the effectiveness of fraud detection. Therefore, according to the findings from the analysis, it can be said that XGBoost is the most effective algorithm for detecting fraudulent transactions.

7. CONCLUSION

In this study, the ability to detect fraudulent transactions in the selected datasets by applying Machine Learning models was analyzed using three different algorithms: Logistic Regression, Random Forest, and XGBoost. The evaluation was based on several evaluation metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, Fraud Detection Efficiency, and False Positive Rate. The results showed noticeable differences between the performance of the selected Machine Learning algorithms.

As shown in the analysis, XGBoost achieved the best performance scores among the other models used. Therefore, XGBoost can be considered the best-performing algorithm for detecting financial fraud. Random Forest also proved to be quite efficient in performing its task, while the use of Logistic Regression was also acceptable although it lagged behind other models. These findings suggest that ensemble-based methods work better than classic classification in fraud detection.

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

To explore whether there is a difference in the performance of selected Machine Learning algorithms for fraud detection, Analysis of Variance was conducted. The results showed significant differences between the selected models. Therefore, we rejected the null hypothesis and concluded that significant differences do exist between the Machine Learning models selected.

From the overall analysis, it was determined that the XGBoost model was the best-suited for detecting fraud, followed by the Random Forest and Logistic Regression models. This research emphasizes the significance of choosing the model for fraud detection and showcases that using ensemble learning algorithms will yield better results in classifying transactions as fraudulent when compared to conventional Machine Learning algorithms.

8. Limitations and Future Scope

The research is associated with some limitations. For one, the analysis was done based on a fraud detection dataset, but since it only includes one set, its limitations might be due to the lack of representation of various fraud patterns from diverse financial companies and digital payment applications. Another limitation is that only three Machine Learning algorithms were considered: Logistic Regression, Random Forest, and XGBoost. These are frequently used in fraud detection studies; however, others could have been taken into account for comparison purposes.

Possible future research could expand the comparative analysis by including other Machine Learning and Deep Learning methods like Support Vector Machines, Artificial Neural Networks, LSTM networks, and ensemble-based approaches. Future research could make use of other fraud detection datasets from various financial areas to enhance the validity of the results obtained. Furthermore, future research could explore real-time fraud detection systems and examine the influence of using different data pre-processing and feature engineering techniques. Such research would add more information regarding the usefulness of ML algorithms for fraud detection purposes.

REFERENCES

1. Aggarwal, C. C. (2015). *Data mining: The textbook*. Springer.
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of FinTech: A new post-crisis paradigm. *Georgetown Journal of International Law, 47*(4), 1271–1319.
3. Bahnsen, A. C., Aouada, D., Ottersten, B., & Stojanovic, A. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134–142.
4. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613.
5. Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.
6. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255.
7. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32.
8. Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
9. Carcillo, F., Le Borgne, Y. A., Caelen, O., Bontempi, G., et al. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences, 557*, 317–331.

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

10. Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794).
11. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. *IEEE Symposium Series on Computational Intelligence*, 159–166.
12. Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review, 96*(1), 108–116.
13. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581–590).
14. George, M. Z. H., Alam, M. K., & Hasan, M. T. (2025). Machine learning for fraud detection in digital banking: A systematic literature review. *arXiv Preprint*.
15. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
16. Hosmer, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied logistic regression* (3rd ed.). Wiley.
17. Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence applications. *Journal of the Academy of Marketing Science, 49*(1), 30–50.
18. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234–245.
19. Kumar, A., & Singh, R. (2022). Cyber fraud and digital payment security in India. *International Journal of Banking and Finance Research, 10*(2), 55–68.
20. McCarthy, J. (1956). Artificial intelligence: Foundational concepts and future directions. Dartmouth Conference Proceedings.
21. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and literature review. *Decision Support Systems, 50*(3), 559–569.
22. Nilsson, N. J. (2010). *The quest for artificial intelligence*. Cambridge University Press.
23. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
24. Sharma, P., & Gupta, N. (2021). Digital banking adoption and cybersecurity challenges in India. *International Journal of Financial Technology, 8*(3), 112–128.
25. Srinivas, V., & Das, S. (2021). Trends in digital payment frauds and preventive measures. *Journal of Banking Security, 15*(2), 75–91.
26. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.
27. Waliullah, M., Rahman, M., & Islam, M. (2025). Assessing cybersecurity threats in digital banking: A systematic review. *arXiv Preprint*.
28. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–66.

ISSN: 2349-6762
Peer Reviewed & Refereed Journal (IF: 7.56)
Journal Website www.nrjbfm.in

29. Reserve Bank of India. (2020–2025). *Annual Reports*. Mumbai: RBI.
30. National Payments Corporation of India. (2020–2025). *Annual Reports*. Mumbai: NPCI.
31. Computer Emergency Response Team–India. (2020–2025). *Annual Reports*. New Delhi: CERT-In.
32. National Cyber Crime Reporting Portal. (2020–2025). *Cyber Crime Statistics Reports*. Government of India.
33. IBM Corporation. (2024). *Cost of a Data Breach Report 2024*.
34. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*.
35. NITI Aayog. (2023). *Artificial Intelligence for Digital Finance and Financial Inclusion in India*.

.