

Evaluating the Effectiveness of Machine Learning Techniques in Detecting Banking Fraud in India

Tushar Kishan Pawar*, Dr. Ujwala Narkhed**

*(Student, Department of MBA, Wainganga college of engineering and management, Nagpur, Maharashtra, India
Email: tp99011@gmail.com)

** (Professor, Department of MBA, Wainganga college of engineering and management, Nagpur, Maharashtra, India
Email : vaidehi1210@gmail.com)

Abstract

Banking fraud has become an important concern in India with the rapid growth of digital banking, electronic payments, and online financial transactions. Machine learning techniques are increasingly being applied to detect fraudulent transactions, but existing studies report different levels of performance because they use different datasets, algorithms, preprocessing methods, class-imbalance treatments, and evaluation measures. This study evaluates the effectiveness of machine learning techniques in detecting banking fraud in India using secondary empirical evidence. Relevant studies were examined and compared with focus on machine-learning techniques, data characteristics, class-imbalance treatment, and fraud-detection performance measures such as precision, recall, F1-score, and AUC. The findings indicate that machine learning demonstrates strong potential for banking fraud detection in India. Random Forest shows strong performance in Indian UPI research, while recent research using data described as actual Indian bank transactions reports strong performance for TabNet. However, the evidence does not support the conclusion that any single machine-learning technique is universally superior. Model effectiveness depends on the nature and quality of the data, preprocessing methods, class imbalance, validation procedures, and evaluation criteria. The study concludes that Indian banks should evaluate machine-learning models using multiple performance measures and consider practical factors such as false positives, interpretability, scalability, and operational requirements. Machine learning should therefore be viewed as an important component of broader banking fraud-risk management rather than as a standalone solution.

Keywords: Banking Fraud, Machine Learning, Fraud Detection, Indian Banking, UPI Fraud, Random Forest, XGBoost, Deep Learning

I. Introduction

The rapid growth of digital banking, internet banking, card transactions, and electronic payment systems has transformed the Indian banking sector. These developments have increased convenience and transaction efficiency, but they have also created greater opportunities for fraudulent activities. According to the Reserve Bank of India (RBI), during 2024–25, card and internet frauds accounted for 13,516 of the 23,953 fraud cases reported by banks and financial institutions, representing 56.5% of reported cases by number. In contrast, frauds relating to advances accounted for 7,950 cases but 92.1% of the total amount involved. The RBI

also notes that frauds reported in a particular year may have occurred in earlier years, highlighting the importance of timely detection and reporting.

Traditional fraud-detection systems generally depend on predefined rules, transaction thresholds, manual investigation, and previously identified fraud patterns. Such approaches remain useful because they are relatively understandable and can be implemented efficiently. However, changing fraud behaviour and the increasing volume of financial transactions have created a need for more adaptive analytical approaches.

Machine learning (ML) offers a data-driven approach to fraud detection by identifying patterns associated with

fraudulent transactions. Techniques such as Logistic Regression, Decision Trees, Random Forest, Support Vector Machines (SVM), XGBoost, neural networks, and other advanced architectures have been widely investigated. A systematic literature review of 93 studies found that SVM and artificial neural networks were among the frequently used techniques, while credit-card fraud was one of the most commonly studied fraud categories.

More recent research confirms that machine learning remains a major area of fraud-detection research. A 2024 review examined 104 studies published between 2012 and 2023 and found continuing growth in the use of machine learning for financial fraud detection. The review also showed substantial variation in fraud types, datasets, algorithms, and evaluation metrics.

Indian research is increasingly focusing on digital-payment fraud, particularly UPI fraud, while newer studies are also investigating advanced deep-learning methods for bank transactions. For example, a 2024 study proposed a hybrid ShuffleNet-SVM approach for UPI fraud detection and reported 95% accuracy. A 2026 study examined five deep-learning architectures, including TabNet, using a Kaggle dataset described by the authors as actual bank transactions in India and reported a ROC-AUC of 0.9739 and accuracy of 97.39% for TabNet.

However, results across studies are difficult to compare directly because researchers use different datasets, fraud types, preprocessing procedures, class-imbalance treatments, validation methods, and performance measures. Therefore, this study focuses on the Indian context and evaluates existing empirical evidence to determine how effective different machine-learning techniques are for banking fraud detection.

II. Problem Statement

Banking fraud is becoming increasingly complex with the rapid growth of digital banking and electronic transactions in India. Although machine learning techniques are increasingly being used to detect fraudulent transactions, existing studies report different results regarding their effectiveness.

These differences arise because researchers use different datasets, machine-learning techniques, preprocessing methods, class-imbalance treatments, and performance measures. In addition, some studies claiming an Indian or India-based research context use simulated or non-Indian datasets, while others use data described as actual Indian banking transactions. This makes direct comparison difficult.

Therefore, there is a need to examine and compare the available empirical evidence on machine-learning

techniques used for banking fraud detection in India and evaluate their effectiveness using appropriate fraud-detection performance measures.

III. Research Objectives

3.1 Main Objective

To evaluate the effectiveness of machine learning techniques in detecting banking fraud in India based on existing empirical evidence.

3.2 Specific Objectives

1. To examine the application of machine learning techniques in banking fraud detection in India.
2. To compare the reported effectiveness of selected machine learning techniques using fraud-detection performance measures.
3. To examine the effect of class imbalance and other methodological factors on machine-learning performance.
4. To identify machine-learning techniques that demonstrate stronger fraud-detection performance across the reviewed evidence.
5. To examine the practical implications of machine-learning-based fraud detection for Indian banks.

IV. Literature Review

4.1 Banking Fraud in India

Banking fraud covers a range of activities involving unauthorized or deceptive use of financial systems, accounts, payment instruments, or transaction information. In the Indian context, digital-payment and card/internet fraud have become particularly important because of the rapid expansion of electronic transactions.

RBI data for 2024–25 show that card/internet frauds represented the largest proportion of reported fraud cases by number, while advances-related frauds represented the largest proportion by amount involved. This difference is important because it shows that fraud frequency and fraud value are not necessarily concentrated in the same banking activities.

The RBI's reporting also shows that fraud reporting and fraud occurrence do not always happen in the same year. This creates an additional challenge for

fraud-risk management because delayed detection can delay corrective action.

4.2 Traditional Fraud Detection

Traditional fraud-detection methods generally rely on fixed rules, predefined thresholds, manual investigation, and expert knowledge. These systems are useful because their decisions can be relatively easy to understand and audit.

However, traditional approaches are generally based on known patterns. When fraudsters change their behaviour, a rule that was effective previously may become less useful. As transaction volumes increase, manual examination and fixed-rule monitoring can also become increasingly difficult to scale.

The literature therefore increasingly examines machine learning as a complementary approach. A 2022 systematic review noted that conventional manual approaches can be costly and time-consuming and documented the growing use of machine learning for financial fraud detection.

4.3 Machine Learning in Fraud Detection

Machine learning allows models to identify patterns from historical data and use those patterns to classify or flag suspicious transactions. The major approaches used in the literature include supervised learning, unsupervised learning, ensemble methods, and deep learning.

A systematic review covering 93 studies found that SVM and artificial neural networks were among the commonly used techniques and that classification-based approaches dominated much of the earlier research.

A later review of 104 studies found continued widespread use of supervised learning and highlighted increasing attention to real datasets, diverse fraud types, and different performance measures.

The Indian literature reflects this broader trend. Recent studies have investigated UPI fraud using conventional classifiers, hybrid models, ensemble methods, and deep-learning architectures.

4.4 Major Machine Learning Techniques

Logistic Regression

Logistic Regression is a relatively simple and interpretable classification technique. It is useful as

a baseline because it allows more complex models to be compared against a straightforward statistical classifier.

Decision Tree

Decision Trees classify observations through a sequence of decision rules. Their structure makes them relatively easy to interpret, although individual trees may become unstable or overfit if not properly controlled.

Random Forest

Random Forest combines multiple decision trees to improve predictive stability. Its ability to handle nonlinear relationships and structured transaction data has made it an important fraud-detection benchmark.

In a 2025 UPI fraud study, Random Forest achieved 96% accuracy, 97% precision, 91% recall, and 93% F1-score.

Support Vector Machine

SVM is a classification method that seeks an effective boundary between classes. It has been applied widely in fraud-detection research and has also been incorporated into hybrid approaches for UPI fraud detection.

A 2024 UPI study combined ShuffleNet with SVM and reported 95% accuracy.

XGBoost

XGBoost is a gradient-boosting technique that has become a strong benchmark for structured classification problems. A 2026 international comparison covering nine fraud methods, nine datasets, and nine evaluation metrics identified XGBoost and Random Forest among the strongest overall methods.

However, strong international benchmark results should not automatically be treated as evidence that the same algorithm is universally superior in India.

Neural Networks and Deep Learning

Neural networks can represent complex nonlinear relationships and have increasingly been used for financial fraud detection.

The 2026 TabNet study evaluated DNN, GRU, LSTM, CNN1D, and TabNet using a dataset

described as actual Indian bank transactions. TabNet produced a ROC-AUC of 0.9739 and accuracy of 97.39%, outperforming the other deep-learning architectures tested in that study.

4.5 Evaluation Metrics

Fraud detection is an imbalanced classification problem, so accuracy alone is not sufficient to determine effectiveness.

Accuracy

Measures the proportion of all transactions classified correctly. It is easy to understand but can be misleading when fraudulent transactions form a small minority.

Precision

Measures the proportion of transactions predicted as fraudulent that are actually fraudulent. Higher precision generally means fewer false alarms.

Recall

Measures the proportion of actual fraudulent transactions that the model successfully detects. Higher recall indicates fewer missed fraud cases.

F1-score

Combines precision and recall into one measure and is useful when both missed fraud and false alerts matter.

ROC-AUC

Measures the ability of a classifier to distinguish between fraudulent and legitimate transactions across classification thresholds.

PR-AUC

Provides a more focused measure of minority-class performance and can be particularly informative for highly imbalanced fraud data.

False-positive rate

Measures the proportion of legitimate transactions incorrectly classified as fraudulent. This has practical importance because excessive false alerts can increase investigation workload and affect legitimate customers.

Recent comparative research emphasizes the importance of evaluating fraud-detection models with multiple metrics instead of relying on one score.

4.6 Class Imbalance

A central challenge in fraud detection is that fraudulent observations are usually much fewer than legitimate observations.

Researchers therefore use techniques such as SMOTE, oversampling, undersampling, and class weighting to address imbalance. The choice of method can influence reported model performance.

The 2026 TabNet study used SMOTE before evaluating five deep-learning architectures and then used three-fold cross-validation for performance assessment.

Similarly, Shah and Sharma (2025) used SMOTE while comparing Logistic Regression, SVM, Decision Tree, Random Forest, and XGBoost on a simulated Sparkov credit-card dataset. Their study found that XGBoost consistently outperformed the other compared algorithms, with precision and recall reaching 99.05% and 99.81%, respectively.

These findings indicate that performance cannot be interpreted independently of the data-balancing procedure.

4.7 Current Research Trends

Several trends are evident in recent research.

First, Indian research increasingly focuses on **UPI and digital-payment fraud**, reflecting the importance of digital transaction security in India.

Second, research increasingly examines **ensemble and hybrid approaches** rather than relying on a single traditional classifier.

Third, **deep-learning architectures** are receiving increased attention. The 2026 TabNet study is an example of this movement toward models designed specifically for structured/tabular transaction data.

Fourth, research is increasingly concerned with **explainability, robustness, and operational usefulness**, rather than predictive accuracy alone. The 2026 international benchmark, for example, explicitly evaluated models across multiple metrics and also considered performance under a business-imposed 5% false-positive-rate constraint.

4.8 Contradictory Findings

The literature does not establish a single universally superior algorithm.

The Indian UPI study reported strong performance for Random Forest, while the 2026 Indian bank-transaction study reported strong performance for TabNet.

At the same time, Shah and Sharma (2025) reported very strong XGBoost performance. However, their dataset was a simulated Sparkov credit-card dataset rather than Indian banking transaction data.

The broader 2026 benchmark likewise found XGBoost and Random Forest to be strong overall, but its findings were based on nine datasets rather than an India-specific banking environment.

These differences suggest that algorithm performance is conditional on the characteristics of the data, preprocessing, class-balancing method, model configuration, and evaluation criteria.

4.9 Research Gap

The existing literature demonstrates strong interest in machine learning for financial fraud detection, and India is one of the prominent countries contributing research in this area. A 2024 review of 104 studies found India among the leading contributors to the research literature.

However, the available Indian evidence remains fragmented. Some studies focus on UPI fraud, others on internal cyber fraud, and newer work examines transaction-level bank fraud using advanced deep-learning models. The underlying datasets and methodological procedures also vary.

An additional problem is that an India-based research paper is not necessarily based on Indian banking data. Shah and Sharma, for example, are affiliated with institutions in Gujarat but explicitly use a simulated Sparkov Kaggle dataset.

Therefore, the research gap is not simply a lack of studies on machine learning and fraud detection. The more relevant gap is the **lack of directly comparable Indian evidence across different machine-learning techniques and evaluation measures**.

This study addresses that gap by distinguishing the underlying data context and comparing the available evidence using common fraud-detection measures and methodological considerations.

V. Methodology

5.1 Research Design

The study adopts a **secondary-data-based comparative research design**. It does not collect responses from customers or employees and does not rely on primary survey data.

Instead, the study evaluates existing empirical research relating to machine-learning-based banking and transaction fraud detection in India.

5.2 Data Sources

The study uses:

- peer-reviewed journal articles;
- academic conference papers;
- published empirical studies;
- systematic literature reviews; and
- official Indian banking and regulatory publications, particularly RBI reports.

Recent research published between 2022 and 2026 is emphasized, while earlier work is considered where it provides useful theoretical or methodological foundations.

5.3 Scope of Evidence

The empirical comparison focuses primarily on **transaction-level and digital-payment fraud**, because this is where the accessible Indian machine-learning evidence is concentrated.

The study therefore does not claim to evaluate every category of banking fraud, such as all loan fraud, money laundering, employee fraud, or financial-statement fraud.

5.4 Study Selection Criteria

Studies are considered relevant when they:

1. examine banking, payment, or financial transaction fraud;
2. apply machine-learning or closely related data-driven methods;
3. have relevance to the Indian banking or digital-payment environment;
4. report empirical findings or measurable model performance; and
5. provide sufficient methodological information to support interpretation.

Studies are excluded when they are purely conceptual, unrelated to fraud detection, duplicate

publications, or lack sufficient evidence for meaningful comparison.

5.5 Data Extraction

For each selected study, the following information is extracted:

Variable	Information recorded
Author and year	Publication details
Fraud type	UPI, card, banking, cyber fraud, etc.
Data source	Dataset or institution
Data context	Indian, synthetic, or other
ML technique	Algorithm/model
Class-imbalance treatment	SMOTE, oversampling, etc.
Validation method	Train/test split, cross-validation, etc.
Performance measures	Accuracy, precision, recall, F1, AUC
Main finding	Principal result
Limitation	Important limitation

5.6 Data Analysis Method

The evidence is analyzed using a **descriptive comparative approach**.

The analysis examines:

- which ML techniques are used;
- how their reported performance differs;
- how class imbalance is handled;
- whether findings are consistent across studies;
- whether differences can be explained by data or methodology; and
- what the findings imply for Indian banking.

Reported performance values are **not averaged into one artificial score**, because the studies use different datasets and experimental conditions.

5.7 Reliability and Validity

Reliability is supported by applying consistent selection and extraction criteria across the selected evidence.

Validity is strengthened by distinguishing between:

- actual Indian transaction data;
- Indian-context but non-verified data;
- simulated or synthetic data; and
- non-Indian benchmark evidence.

This distinction prevents strong performance on a synthetic or foreign dataset from being incorrectly presented as evidence about Indian banks.

VI. Analysis and Findings

6.1 Profile of Selected Evidence

The selected evidence demonstrates growing use of ML for fraud detection in the Indian banking and digital-payment environment.

Table 6.1: Selected Studies

Study	Year	Data / Context	Techniques	Main reported result
Roy & Prabhakaran	2022/2023	Internal cyber fraud in Indian banks	K-NN and ML-supported fraud-risk framework	Developed an approach for identifying, prioritizing and predicting internal cyber-fraud risks.
Tamilselvi et al.	2024	UPI fraud	ShuffleNet + SVM	Reported 95% accuracy.
Sethi et al.	2025	UPI fraud	Decision Tree, SVM, Random Forest, Logistic Regression and ensembles	Random Forest reported 96% accuracy, 97% precision, 91% recall and 93% F1-score.
Shah & Sharma	2025	Simulated Sparkov credit-card dataset	Logistic Regression, SVM, Decision Tree, Random Forest, XGBoost	XGBoost produced the strongest results; precision reached 99.05% and recall 99.81%.
Prashanth et al.	2026	Kaggle dataset described as actual bank transactions in India	DNN, GRU, LSTM, CNN1D, TabNet	TabNet achieved ROC-AUC 0.9739 and accuracy 97.39%.

Sources: Roy & Prabhakaran; Tamilselvi et al.; Sethi et al.; Shah & Sharma; Prashanth et al.

6.2 Comparison of Machine Learning Techniques

The findings demonstrate strong performance from several different types of models.

Random Forest is a particularly strong conventional approach in the Indian UPI evidence. Sethi et al. reported 96% accuracy, 97% precision, 91% recall, and 93% F1-score.

The 2024 UPI study used a hybrid architecture combining ShuffleNet and SVM and reported 95% accuracy. This

suggests that combining feature extraction with classification can provide strong performance in payment-fraud detection.

The 2026 TabNet study reported ROC-AUC of 0.9739 and accuracy of 97.39%, outperforming the other deep-learning architectures tested on its Indian transaction dataset.

The Shah and Sharma study reported stronger XGBoost results than the other algorithms it compared, but because the dataset was simulated rather than Indian banking data, the finding should be treated as supporting methodological evidence rather than direct evidence about Indian banks.

6.3 Effect of Data and Methodological Differences

The reported results cannot be interpreted solely as differences in algorithm quality.

The studies vary in:

- dataset source;
- fraud definition;
- sample characteristics;
- feature preparation;
- class-balancing procedure;
- validation approach; and
- performance measures.

For example, the TabNet study applied SMOTE and three-fold cross-validation, while Shah and Sharma used SMOTE and multiple train-test ratios with ten-fold cross-validation.

Consequently, a model producing 97% accuracy in one study cannot automatically be regarded as inferior or superior to a model producing 95% accuracy in another study.

6.4 Effect of Class Imbalance

Class imbalance is a major factor affecting fraud-detection results.

The TabNet study used SMOTE to balance the classes before evaluating its models. Shah and Sharma also used SMOTE before comparing their five classifiers.

This demonstrates that the reported effectiveness of an ML technique depends partly on how the dataset is prepared. Therefore, model performance must always be interpreted together with the imbalance-treatment method.

6.5 Key Findings

Finding 1: Machine learning demonstrates strong potential

The reviewed Indian evidence shows that ML can identify fraudulent transaction patterns with strong predictive performance.

Finding 2: Random Forest is a strong conventional benchmark

The UPI study produced strong precision, recall, F1-score, and accuracy results using Random Forest.

Finding 3: Advanced deep learning is increasingly competitive

The TabNet study achieved strong ROC-AUC and accuracy and reported advantages in interpretability and false-positive/false-negative reduction.

Finding 4: XGBoost is highly competitive, but context matters

XGBoost performed strongly in the Shah–Sharma study, but that evidence came from a simulated dataset.

Finding 5: No universal best technique can be established

The available evidence does not justify declaring one algorithm universally superior for Indian banking fraud detection.

6.6 Findings Against Research Objectives

Research Objective	Finding
Examine ML application in Indian fraud detection	ML is increasingly used in banking, UPI, digital-payment and cyber-fraud detection.
Compare selected techniques	Random Forest, hybrid models, XGBoost and advanced deep-learning methods all demonstrate strong performance in different studies.
Examine class imbalance	Balancing techniques materially influence reported results.
Identify stronger-performing approaches	Random Forest and TabNet demonstrate strong results in Indian-context evidence, but no universal winner can be established.
Examine practical implications	Banks need to consider predictive performance together with false positives, interpretability, scalability, and operational requirements.

6.7 Overall Finding

The overall evidence indicates that **machine learning is an effective and promising approach to banking fraud**

detection in India, but its effectiveness is conditional rather than universal.

The principal determinants of reported performance include the type and quality of data, class-imbalance treatment, preprocessing, model architecture, validation procedure, and choice of evaluation metric.

VII. Conclusion

This study evaluated the effectiveness of machine-learning techniques in detecting banking fraud in India using existing empirical evidence.

The findings demonstrate that machine learning has significant potential for strengthening fraud detection in India's banking and digital-payment environment. Random Forest shows strong performance in Indian UPI research, while recent research using a dataset described as actual Indian bank transactions reports strong results for TabNet.

However, the evidence does not support the conclusion that one machine-learning technique is universally superior. Performance varies according to the dataset, fraud type, preprocessing method, class-imbalance treatment, validation procedure, and evaluation criteria. The study therefore finds that the effectiveness of machine learning should be evaluated as a **multidimensional concept rather than through a single accuracy score.**

Class imbalance is particularly important. Because fraudulent transactions generally represent a minority of observations, accuracy alone may give an incomplete picture of model performance. Precision, recall, F1-score, AUC, and false-positive behaviour provide more meaningful information about whether a model can detect fraud while limiting unnecessary alerts.

The study also identifies an important distinction between **technical performance and practical banking effectiveness.** A highly accurate model may still be difficult to implement, expensive to operate, difficult to interpret, or prone to excessive false alerts. Therefore, banks should consider both predictive performance and operational requirements when selecting fraud-detection systems.

Overall, the study concludes that machine learning should be regarded as an important component of banking fraud-risk management in India, but model selection should be based on the characteristics of the data, fraud environment, evaluation requirements, and operational needs of the financial institution rather than on a universal ranking of algorithms.

Recommendations

1. Indian banks should evaluate ML models using multiple performance measures rather than accuracy alone.
2. Class imbalance should be explicitly addressed during fraud-detection model development and evaluation.
3. Banks should consider false positives, interpretability, scalability, and investigation workload when selecting ML models.
4. Machine learning should complement existing rules, transaction monitoring, and human investigation rather than completely replace them.
5. Fraud-detection models should be continuously monitored and updated because fraud patterns can change over time.

Limitations

The study is based on secondary empirical evidence, and the reviewed studies use different datasets, fraud definitions, preprocessing procedures, and validation methods. These differences limit direct numerical comparison.

In addition, some studies use simulated or synthetic datasets. Consequently, their findings should not automatically be generalized to the entire Indian banking sector.

The available Indian literature is also concentrated in particular areas, especially digital-payment and transaction fraud, meaning that the findings should not be interpreted as covering every type of banking fraud.

Future Research

Future research should examine larger and more consistently documented Indian banking datasets and compare machine-learning techniques under standardized experimental conditions. Further research should also investigate real-time fraud detection, explainable AI, adaptive learning, concept drift, privacy-preserving machine learning, and fraud detection across different Indian payment channels.

References

- 1) Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637. DOI: 10.3390/app12199637

- 2) Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, 1130. DOI: 10.1057/s41599-024-03606-0
- 3) Prashanth, B. S., Kumar, M., Hoque, A., Al Muraqab, N., Moonesar, I. A., Braendle, U. C., & Rao, A. (2026). Prediction of bank transaction fraud using TabNet—an adaptive deep learning architecture. *International Review of Economics & Finance*, 106, 104916. DOI: 10.1016/j.iref.2026.104916
- 4) Roy, N. C. (2022/2023). Internal-led cyber frauds in Indian banks: An effective machine learning-based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, 75(2), 246–296. DOI: 10.1108/AJIM-11-2021-0339
- 5) Sethi, B., Mhatre, S., Yadav, S., Das, S., & Jadhav, V. (2025). Machine learning-based UPI fraud detection: A comprehensive approach using Random Forest. In *Proceedings of the MULTINOVA: First International Conference on Artificial Intelligence in Engineering, Healthcare and Sciences*, 462–470. DOI: 10.2991/978-94-6463-852-3_29
- 6) Shah, D., & Sharma, L. K. (2025). Contrastive study of machine learning techniques for credit card fraud detection. *Indian Journal of Science and Technology*, 18(16), 1248–1259. DOI: 10.17485/IJST/v18i16.572
- 7) Tamilselvi, M., Srinivasan, T. S., Begum, R., Krishnamoorthi, K., Giri, J., et al. (2024). Experimental evaluation Unified Payment Interface (UPI) fraud detection system using elevated deep learning methodology. In *2024 2nd International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*. DOI: 10.1109/ICETEMS64039.2024.10965083
- 8) Yapp, E. K. Y., & Yeh, H.-Y. (2026). An extensive experimental comparison of machine and deep learning methods for credit and bank fraud detection. *Finance Research Letters*, 88, 109190. DOI: 10.1016/j.frl.2025.109190
- 9) Reserve Bank of India. (2025). *Annual Report 2024–25*.