ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

ARTIFICIAL INTELLIGENCE-BASED FRAUD DETECTION IN DIGITAL BANKING: A COMPARATIVE MACHINE LEARNING APPROACH ANOMALY DETECTION, ENSEMBLE ML BANKING, FINTECH, FRAUD PREVENTION

Dr. Nawaz Ali Hamdulay[1], Dr. Sameer Mohammed Hussain Shaikh[2]
[1]Founder & Director, Infomania IT and Management Academy LLP), (B.E, M.E, MMS - IT, PhD-JJTU) India
Email id: nawaz.hamdulay@gmail.com, ORCID iD: 0009-0007-7377-9990
[2]Principal [IC], St. Peter Degree College, Vasia, India, (B. Com, M. Com, MBA-Finance, Phd JJTU) India
Email id: smshaikh2010@gmail.com, ORCID iD: 0009-0004-1660-325X

KEYWORDS: Artificial Intelligence, Machine Learning, Digital Banking, Fraud Detection, Anomaly Detection, Ensemble Learning, Fintech, Fraud Prevention, Random Forest, Gradient Boosting, Isolation Forest, Financial Transactions.

ABSTRACT

The rapid growth of digital banking, mobile payments, internet banking, and fintech platforms has transformed the financial services industry while simultaneously increasing exposure to fraudulent activities. Traditional rule-based fraud detection systems often struggle to identify sophisticated, rapidly evolving, and previously unseen fraud patterns. Artificial Intelligence (AI) and Machine Learning (ML) provide promising solutions by enabling financial institutions to analyze large volumes of transactional data, detect anomalous behaviour, and continuously improve fraud identification. This research examines an AI-based approach to fraud detection in digital banking through a comparative analysis of machine learning techniques, with particular emphasis on anomaly detection and ensemble learning. Supervised algorithms such as Logistic Regression, Decision Tree, Random Forest, and Gradient Boosting are considered alongside anomaly-detection techniques such as Isolation Forest. The proposed methodology involves data preprocessing, feature engineering, class-imbalance handling, model training, and evaluation using accuracy, precision, recall, F1-score, Area Under the Receiver Operating Characteristic Curve (ROC-AUC), and fraud-detection rate. Because banking fraud datasets are typically highly imbalanced, the study emphasizes precision and recall rather than accuracy alone. The research proposes that ensemble machine learning models can provide more robust fraud detection than individual classifiers by combining multiple decision mechanisms and capturing complex nonlinear transaction patterns. The study further highlights the importance of explainability, real-time detection, data privacy, and adaptability in practical fintech environments. The proposed comparative framework can assist banks and fintech organizations in selecting appropriate AI techniques for reducing financial losses while maintaining legitimate customer transactions.

INTRODUCTION

The digital transformation of the banking sector has fundamentally changed the way customers access and use financial services. Internet banking, mobile banking applications, digital wallets, instant payments, card transactions, and fintech platforms have increased the speed and convenience of financial transactions. However, this rapid digitalization has also created new opportunities for cybercriminals and fraudsters. Fraudulent transactions may involve stolen credentials, account takeover, payment manipulation, identity theft, card fraud, synthetic identities, and other forms of financial abuse.

Traditional fraud prevention systems generally rely on predefined rules. For example, a transaction may be flagged when it exceeds a particular monetary threshold, originates from an unusual geographic location, or occurs after a certain number of failed authentication attempts. Although rule-based systems are relatively easy to implement and interpret, they have significant limitations. Fraudsters can modify their behaviour to circumvent known rules, while legitimate transactions may be incorrectly classified as suspicious. Furthermore, manually creating and maintaining large collections of rules becomes increasingly difficult as transaction volumes and fraud techniques grow.

Artificial Intelligence offers an alternative approach by enabling automated systems to identify relationships and behavioural patterns within large datasets. Machine learning algorithms can learn from historical transactions and identify characteristics associated with fraudulent behaviour. In supervised learning, models are trained using transactions labelled as fraudulent or legitimate. In contrast, unsupervised and semi-supervised approaches attempt to identify unusual transactions without requiring complete fraud labels.

Anomaly detection is particularly relevant to digital banking because fraudulent transactions may differ significantly from a customer's normal behavioural profile. An anomaly-detection model can identify unusual transaction amounts, frequencies, locations, device characteristics, or temporal patterns. This is important for detecting emerging fraud that may not resemble previously observed cases.

Another important AI approach is ensemble learning. Ensemble models combine the outputs of multiple decision trees or different learning mechanisms to improve predictive performance. Algorithms such as Random Forest and Gradient Boosting can model nonlinear relationships among transaction characteristics and may be more robust than individual classification algorithms.

The central purpose of this research is therefore to develop a comparative machine learning framework for AI-based fraud detection in digital banking. The study considers both conventional classification and anomaly-detection techniques and evaluates their suitability for fraud prevention. The research particularly investigates whether ensemble learning techniques can improve the identification of fraudulent transactions while reducing false positives.

The study is relevant to commercial banks, digital banks, payment service providers, and fintech organizations seeking scalable and adaptive fraud-prevention systems. An effective AI-based fraud detection system should not only achieve high predictive performance but also operate efficiently in near real time, preserve customer trust, and provide sufficient interpretability for compliance and operational decision-making.

LITERATURE REVIEW

Al-Bulushi et al. [2026], the authors investigate the application of supervised machine learning algorithms and ensemble models for improving credit card fraud detection. The study addresses the growing challenge of identifying fraudulent transactions within highly imbalanced and complex financial datasets. The authors evaluate multiple supervised learning techniques and ensemble approaches to determine their effectiveness in distinguishing legitimate transactions from fraudulent activities. Their findings demonstrate that machine learning-based methods can enhance fraud detection performance by identifying patterns that may be difficult to detect through traditional rule-based systems. Ensemble models are particularly valuable because they combine the predictive strengths of multiple algorithms, potentially improving accuracy, robustness, and generalization. The study highlights the importance of selecting appropriate performance measures for fraud detection, where false negatives and false positives have different financial consequences. Al-Bulushi et al. (2026) provide evidence that supervised and ensemble learning approaches can strengthen automated credit card fraud detection and support more reliable financial security systems [15].

Thivaios et al. [2026], the authors provide a comprehensive survey of machine learning (ML) and deep learning (DL) techniques used for financial fraud detection. The study examines different model architectures, data modalities, and practical challenges associated with deploying fraud detection systems in real-world financial environments. The authors emphasize that financial fraud is increasingly complex, requiring advanced computational methods capable of identifying subtle and evolving patterns within large-scale transactional data. The review highlights the effectiveness of both traditional ML algorithms and DL architectures in detecting fraudulent activities, while also discussing challenges such as highly imbalanced datasets, changing fraud patterns, data quality, interpretability, and computational requirements. Particular attention is given to the gap between high-performing models developed in research settings and their practical implementation in financial institutions. Thivaios et al. (2026) demonstrate that successful fraud detection requires not only accurate predictive models but also adaptable, explainable, scalable, and deployment-ready solutions capable of responding to emerging financial threats [19].

Ahmed et al. [2025], the authors propose a credit card fraud detection approach that combines ensemble machine learning classifiers with hybrid data sampling techniques. The study addresses a major challenge in fraud detection: the severe class imbalance between legitimate and fraudulent transactions, which can negatively affect the performance of conventional machine learning models. By applying hybrid sampling methods, the authors aim to create a more balanced training dataset while retaining important characteristics of the original transaction data. The use of ensemble learning further strengthens fraud detection by combining multiple classifiers to improve predictive performance and reduce the limitations of individual algorithms. The approach demonstrates the importance of integrating effective data-preprocessing strategies with advanced machine learning techniques

when dealing with imbalanced financial datasets. Ahmed et al. (2025) highlight that combining hybrid sampling and ensemble classification can improve the identification of fraudulent transactions and provide a more reliable framework for automated credit card fraud detection in practical financial applications [12].

Shih et al. [2025], the authors examine fund transfer fraud detection by combining self-attention mechanisms with graph neural networks (GNNs). The study addresses the limitations of conventional fraud detection methods, particularly their difficulty in capturing irregular transaction patterns and complex relationships among customers and financial accounts. By representing financial transactions and customer interactions as graphs, GNNs can identify suspicious relationships and structural patterns that may not be evident from individual transactions. The integration of self-attention enables the model to focus on important transactional and relational features, improving its ability to distinguish legitimate activities from fraudulent behaviour. This approach is particularly relevant to modern financial systems, where fraud can involve interconnected accounts and coordinated transaction activities. The study demonstrates the potential of combining advanced deep learning architectures with relational data for more effective fraud detection. Shih et al. (2025) contribute to the literature by highlighting how attention-based GNN models can improve the detection of complex and irregular financial fraud [14].

OBJECTIVES

1. To examine the role of Artificial Intelligence and Machine Learning in digital banking fraud prevention.
2. To compare supervised machine learning algorithms such as Logistic Regression, Decision Tree, Random Forest, and Gradient Boosting for identifying fraudulent transactions.
3. To investigate the effectiveness of anomaly detection, particularly Isolation Forest, in identifying unusual and potentially fraudulent banking transactions.
4. To evaluate the impact of ensemble learning on fraud-detection performance.
5. To address the problem of highly imbalanced banking transaction datasets through appropriate preprocessing and resampling techniques.
6. To compare machine learning models using accuracy, precision, recall, F1-score, ROC-AUC, and fraud-detection rate.
7. To identify the trade-off between fraud detection and false-positive rates.
8. To examine the practical requirements for implementing AI-based fraud detection in banking and fintech environments, including scalability, explainability, real-time processing, and adaptability.
9. To propose a machine learning-based framework that can support proactive fraud prevention in digital banking.

HYPOTHESIS

The study proposes the following hypotheses:

H1: Machine Learning Performance Hypothesis

Machine learning-based fraud detection models significantly improve the identification of fraudulent digital banking transactions compared with conventional rule-based approaches.

H2: Ensemble Learning Hypothesis

Ensemble machine learning algorithms, particularly Random Forest and Gradient Boosting, achieve higher fraud-detection performance than individual classification algorithms such as Logistic Regression and Decision Tree.

H3: Anomaly Detection Hypothesis

Anomaly-detection techniques such as Isolation Forest can identify previously unseen or unusual fraudulent transaction patterns that may not be effectively detected by supervised classification models.

H4: Class-Imbalance Hypothesis

Appropriate handling of class imbalance through techniques such as class weighting, under sampling, or synthetic oversampling significantly improves the recall and F1-score of machine learning fraud-detection models.

H5: False-Positive Hypothesis

Models that incorporate behavioural and transaction-level features can reduce false-positive rates while maintaining high fraud-detection performance compared with models based primarily on transaction amount and basic transaction attributes.

H6: Combined Detection Hypothesis

A hybrid fraud-detection framework combining supervised ensemble learning with anomaly detection provides more comprehensive fraud prevention than either approach operating independently.

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

RESEARCH METHODOLOGY

❖ Research Design

This research adopts a quantitative and experimental research design. A comparative machine learning approach will be used to evaluate multiple algorithms for digital banking fraud detection. The research will consist of data collection, data preprocessing, exploratory analysis, feature engineering, model development, model training, performance evaluation, and comparative analysis.

The proposed framework is designed to evaluate both supervised classification and anomaly-detection approaches.

❖ Dataset

The study can utilize a publicly available financial transaction fraud dataset or an anonymized banking transaction dataset obtained from an appropriate research or financial institution.
The dataset should ideally contain transaction-level variables such as:

- Transaction amount
- Transaction date and time
- Transaction type
- Merchant or transaction category
- Customer/account characteristics
- Geographic information
- Device characteristics
- Authentication-related variables
- Historical transaction behaviour
- Fraud/non-fraud classification

The target variable will identify whether a transaction is legitimate or fraudulent.
Because actual banking datasets contain sensitive customer information, personally identifiable information should be removed or anonymized before analysis.

❖ Data Preprocessing

Data preprocessing is essential for producing reliable machine learning results. The following procedures will be applied:

Missing-Value Treatment
Missing values will be identified and treated using appropriate statistical or model-based techniques. Numerical variables may be imputed using median values, while categorical variables may be assigned the most frequent category or an explicit unknown category.

Data Cleaning
Duplicate transactions, invalid records, inconsistent data types, and impossible values will be examined and corrected or removed where appropriate.

Categorical Encoding
Categorical features such as transaction type and merchant category will be transformed into numerical representations using techniques such as one-hot encoding or target encoding, depending on the selected model.

Feature Scaling
Scaling will be applied where required. Standardization or normalization may be used for algorithms sensitive to feature magnitude, while tree-based algorithms generally require less scaling.

❖ Feature Engineering

Feature engineering will be used to improve the ability of models to identify fraudulent behaviour.
Potential features include:

- Transaction amount deviation from a customer's historical average
- Number of transactions within a specified time interval
- Time since the customer's previous transaction

- Transaction frequency
- Geographic distance between consecutive transactions
- New-device indicator
- New-merchant indicator
- Unusual transaction-time indicator
- Customer spending-pattern deviation
- Failed authentication frequency
- Historical fraud-risk score

Behavioural features are particularly important because fraud detection is not simply a matter of determining whether a transaction is statistically unusual. A transaction should be evaluated in the context of the customer's historical behaviour.

❖ **Handling Class Imbalance**

Fraud datasets are usually highly imbalanced, with legitimate transactions substantially outnumbering fraudulent transactions. Directly training a model on such data may cause it to favour the majority class.
The study will therefore investigate techniques such as:

- Class-weighted learning
- Random under sampling
- Random oversampling
- Synthetic Minority Over-sampling Technique (SMOTE)
- Threshold optimization

The selected approach will be determined based on experimental results and validation performance.

❖ **Machine Learning Models**

The study will compare the following algorithms:

Model	**Category**	**Expected Strength**
Logistic Regression	Supervised classification	Interpretability and baseline performance
Decision Tree	Supervised classification	Simple nonlinear decision rules
Random Forest	Ensemble learning	Robustness and nonlinear pattern detection
Gradient Boosting	Ensemble learning	High predictive performance
Isolation Forest	Anomaly detection	Detection of unusual/novel patterns

Table 1

Logistic Regression will serve as a baseline model. Decision Tree will provide a simple nonlinear classifier. Random Forest and Gradient Boosting will represent ensemble approaches. Isolation Forest will represent unsupervised anomaly detection.

❖ **Model Training**

The dataset will be divided into training, validation, and testing subsets. A possible configuration is:

- 70% training data
- 15% validation data
- 15% testing data

Stratified sampling should be used for supervised classification to preserve the proportion of fraudulent transactions across subsets.
Cross-validation can additionally be employed during model selection and hyperparameter tuning. Care must be taken to prevent data leakage, particularly when transaction records are time-dependent.

❖ **Anomaly Detection Framework**

Isolation Forest will be trained to identify transactions that deviate from expected transaction patterns.
The anomaly score generated by the model can be incorporated into the overall fraud-risk assessment. Transactions with high anomaly scores can be sent for additional verification or combined with the output of supervised classification models.

A hybrid system can therefore operate as follows:
Transaction → Data Preprocessing → Feature Engineering → Supervised Model + Anomaly Detector → Risk Score → Decision
The final decision may classify a transaction as:

- Legitimate
- Suspicious—manual review required
- High-risk—transaction blocked or additional authentication required

This approach allows anomaly detection to complement rather than replace supervised fraud classification.

❖ Evaluation Metrics

Because fraud detection is an imbalanced classification problem, several evaluation metrics will be used.

Accuracy

Accuracy represents the proportion of correctly classified transactions:
Accuracy = (TP + TN) / (TP + TN + FP + FN)
However, accuracy alone is not sufficient because a model can achieve high accuracy while detecting very few fraudulent transactions.

Precision

Precision measures the proportion of transactions classified as fraudulent that are actually fraudulent:
Precision = TP / (TP + FP)
High precision is important because excessive false alerts increase operational costs and can negatively affect customer experience.

Recall

Recall measures the proportion of actual fraudulent transactions that are successfully detected:
Recall = TP / (TP + FN)
Recall is particularly important in fraud prevention because missed fraudulent transactions can result in financial losses.

F1-Score

The F1-score provides a balance between precision and recall:
F1 = 2 × (Precision × Recall) / (Precision + Recall)

ROC-AUC

The Area Under the Receiver Operating Characteristic Curve will be used to evaluate the model's ability to distinguish fraudulent from legitimate transactions across different classification thresholds.

False-Positive Rate

The false-positive rate will also be examined because incorrectly blocking legitimate banking transactions can reduce customer satisfaction and create unnecessary investigation costs.

❖ Comparative Analysis

The performance of all models will be compared using the selected evaluation metrics. Particular attention will be given to:

1. Fraud detection capability.
2. False-positive rate.
3. Performance on imbalanced data.
4. Computational efficiency.
5. Interpretability.
6. Ability to detect previously unseen patterns.
7. Suitability for real-time banking applications.

A comparative table can be used to determine which algorithm provides the best balance between fraud detection and operational requirements.

❖ Proposed Hybrid AI Fraud Detection Model

Based on the comparative analysis, the research proposes a hybrid fraud detection architecture combining supervised ensemble learning and anomaly detection.
The conceptual architecture is:

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

Customer Transaction Data
↓
Data Cleaning & Preprocessing
↓
Feature Engineering
↓
Class-Imbalance Management
↓
Parallel Detection Layer
→ Random Forest
→ Gradient Boosting
→ Isolation Forest
↓
Risk-Score Aggregation
↓
Fraud Decision Engine
↓
Legitimate / Suspicious / Fraudulent
↓
Continuous Model Monitoring & Retraining

The ensemble models provide supervised fraud classification, while Isolation Forest contributes an anomaly score that can help identify unusual transactions. Combining these signals can potentially improve the detection of both known and emerging fraud patterns.

- **Ethical and Security Considerations**

AI-based fraud detection must consider privacy, fairness, transparency, and security. Banking datasets contain sensitive financial information, so data should be anonymized and handled according to applicable data-protection requirements.

Model bias must also be monitored. A model should not systematically generate excessive false positives for particular customer groups because of inappropriate or proxy features.

Explainability is another important consideration. Financial institutions may need to understand why a transaction was assigned a high-risk score. Techniques such as feature importance and explainable AI methods can assist investigators in interpreting model predictions. Finally, fraud-detection models themselves can become targets for adversarial manipulation. Continuous monitoring, model validation, access controls, and periodic retraining are therefore necessary components of a secure AI-based fraud prevention system.

ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN DIGITAL BANKING FRAUD PREVENTION

The rapid growth of digital banking, mobile payments, internet transactions, and online financial services has increased both the volume and complexity of financial fraud. Traditional rule-based fraud detection systems often struggle to identify rapidly changing and sophisticated fraudulent behaviour because they depend on predefined patterns and rules. Artificial Intelligence (AI) and Machine Learning (ML) provide more adaptive approaches by analysing large volumes of transactional data and identifying unusual patterns in real time (Al-Hashedi & Magalingam, 2021).

ML plays a particularly important role in digital banking fraud prevention because algorithms can learn from historical transaction data and distinguish between legitimate and fraudulent activities. Supervised learning techniques, including decision trees, support vector machines, random forests, and neural networks, can classify transactions according to previously identified fraud patterns. Unsupervised learning can additionally identify anomalies without requiring every fraudulent pattern to be labelled in advance, making it useful for detecting emerging forms of fraud (Hafez et al., 2025).

AI systems can also strengthen fraud prevention through real-time behavioural analysis. By examining transaction amount, location, device information, transaction frequency, and customer behaviour, AI models can identify

deviations from normal activity and generate alerts before substantial financial losses occur. Recent research demonstrates that ensemble and deep-learning approaches can improve detection performance, particularly when dealing with highly imbalanced transaction datasets in which legitimate transactions greatly outnumber fraudulent ones (Al-Bulushi et al., 2026).

However, the effectiveness of AI and ML depends on data quality, model transparency, privacy, and continuous adaptation. Fraudsters continually change their techniques, creating the problem of concept drift and requiring models to be regularly updated. Furthermore, highly complex AI models may be difficult for banks and regulators to interpret. Explainable AI can therefore improve transparency by helping institutions understand why particular transactions are classified as suspicious (Khoozani et al., 2026).

AI and ML are transforming digital banking fraud prevention from reactive rule-based monitoring toward proactive, adaptive, and real-time risk detection. Their effective implementation can improve fraud detection accuracy, reduce financial losses, and strengthen customer trust, provided that banks address issues relating to data imbalance, privacy, explainability, and continuous model monitoring.

COMPARE SUPERVISED MACHINE LEARNING ALGORITHMS SUCH AS LOGISTIC REGRESSION, DECISION TREE, RANDOM FOREST, AND GRADIENT BOOSTING FOR IDENTIFYING FRAUDULENT TRANSACTIONS

Algorithm	Type	Key Features	Advantages	Limitations	Suitability for Fraud Detection
Logistic Regression	Linear classification	Uses a linear decision boundary to classify transactions	Simple, fast, interpretable, easy to implement	May struggle with complex, non-linear patterns	Good baseline model; useful when interpretability is important
Decision Tree	Tree-based classification	Splits data based on feature values to make decisions	Easy to understand, handles non-linear relationships, requires little preprocessing	Can easily overfit the training data	Good for identifying understandable fraud patterns
Random Forest	Ensemble of decision trees	Combines predictions from multiple decision trees	High accuracy, reduces overfitting, handles complex relationships	Less interpretable and computationally heavier than a single tree	Very suitable for fraud detection due to strong predictive performance
Gradient Boosting	Ensemble learning	Builds trees sequentially, with each tree correcting previous errors	High predictive accuracy, captures complex patterns, effective with structured data	More computationally intensive and sensitive to parameter settings	Highly suitable for detecting sophisticated and complex fraudulent transactions

Table 2

Comparison Criteria

Criteria	Logistic Regression	Decision Tree	Random Forest	Gradient Boosting
Accuracy	Moderate	Moderate–High	High	Very High
Interpretability	High	High	Moderate	Low–Moderate
Handles Non-linearity	Low	High	High	High
Overfitting Risk	Low	High	Low	Moderate
Training Speed	Fast	Fast	Moderate	Slower
Fraud Detection Performance	Good	Good	Excellent	Excellent

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

Criteria	Logistic Regression	Decision Tree	Random Forest	Gradient Boosting
Best Use	Baseline & interpretable results	Simple decision rules	Robust classification	Maximum predictive performance

Table 3

EFFECTIVENESS OF ANOMALY DETECTION, PARTICULARLY ISOLATION FOREST, IN IDENTIFYING UNUSUAL AND POTENTIALLY FRAUDULENT BANKING TRANSACTIONS

Anomaly detection plays an important role in identifying unusual and potentially fraudulent banking transactions, particularly when fraudulent activities are rare and difficult to detect using conventional classification techniques. Unlike supervised learning methods that require large amounts of labelled fraudulent transaction data, anomaly-detection techniques can identify transactions that significantly deviate from normal banking behaviour. This makes them particularly useful in real-world fraud-detection systems, where new and previously unseen fraud patterns may emerge.

Among various anomaly-detection algorithms, Isolation Forest is an effective method for detecting suspicious banking transactions. The algorithm works by randomly selecting features and splitting values to isolate individual observations. Since unusual transactions tend to differ substantially from normal transactions, they are generally isolated more quickly than regular transactions. Isolation Forest assigns an anomaly score to each transaction, with transactions receiving higher anomaly scores being considered more likely to be anomalous or potentially fraudulent.

The effectiveness of Isolation Forest can be evaluated using measures such as precision, recall, F1-score, ROC-AUC, and the false-positive rate. Recall is particularly important because failing to identify fraudulent transactions can result in significant financial losses. At the same time, precision and the false-positive rate must also be considered because incorrectly flagging legitimate transactions can cause customer inconvenience and increase the workload of fraud-investigation teams [16].

Isolation Forest is especially valuable when transaction datasets are highly imbalanced or when labelled fraud examples are limited. It can analyse large volumes of transaction data and identify unusual patterns based on characteristics such as transaction amount, transaction frequency, location, time, and spending behaviour. However, its performance depends heavily on appropriate feature selection, parameter configuration, and the definition of what constitutes normal behaviour. Legitimate transactions that are naturally unusual may also be incorrectly classified as anomalies.

Overall, Isolation Forest provides an efficient and flexible approach for identifying unusual banking transactions and can complement supervised fraud-detection models. Its ability to detect previously unseen patterns makes it particularly useful as an additional layer of fraud monitoring. Nevertheless, anomaly scores should ideally be combined with other risk indicators and machine-learning techniques to reduce false positives and improve the reliability of fraud detection. Thus, Isolation Forest can contribute significantly to a comprehensive banking fraud-detection framework.

IMPACT OF ENSEMBLE LEARNING ON FRAUD-DETECTION PERFORMANCE

Fraud detection is a critical challenge in financial institutions, e-commerce platforms, insurance companies, and digital payment systems. The increasing volume and complexity of fraudulent transactions have created a need for machine-learning techniques that can accurately identify suspicious activities. Ensemble learning is an effective approach because it combines the predictions of multiple machine-learning models to improve overall classification performance. Evaluating its impact on fraud-detection performance involves comparing ensemble methods with individual classifiers using appropriate performance measures.

Ensemble learning methods such as Random Forest, AdaBoost, Gradient Boosting, XGBoost, and voting or stacking classifiers can provide better fraud-detection results than a single machine-learning model. By combining several learners, ensemble techniques can reduce prediction errors, improve model stability, and capture complex patterns in transaction data. This is particularly useful for fraud detection because fraudulent transactions are often rare and may have characteristics that differ significantly from legitimate transactions.

The performance of ensemble models should be evaluated using metrics such as accuracy, precision, recall, F1-score, and area under the Receiver Operating Characteristic curve (ROC-AUC) [17]. However, accuracy alone may be misleading because fraud datasets are usually highly imbalanced. For example, a model could achieve high accuracy simply by classifying most transactions as legitimate while failing to detect actual fraud. Therefore, recall is especially important because it measures the proportion of fraudulent transactions correctly identified. Precision is also significant because a high number of false positives can inconvenience legitimate customers and increase investigation costs.

A comparative evaluation can involve training individual algorithms, such as logistic regression, decision trees, or support vector machines, and then comparing their results with ensemble models under the same dataset and experimental conditions. Cross-validation can further improve the reliability of the evaluation by testing model performance across multiple data subsets [10].

Ensemble learning generally has a positive impact on fraud-detection performance by improving predictive accuracy, robustness, and the ability to detect complex fraudulent patterns. Nevertheless, ensemble models can require greater computational resources and may be less interpretable than simpler algorithms. Consequently, the most effective fraud-detection system should balance detection performance, computational efficiency, interpretability, and the operational cost of false positives and false negatives.

THE PROBLEM OF HIGHLY IMBALANCED BANKING TRANSACTION DATASETS THROUGH APPROPRIATE PREPROCESSING AND RESAMPLING TECHNIQUES

One of the major challenges in developing effective machine learning-based fraud detection systems is the highly imbalanced nature of banking transaction datasets. In a typical digital banking environment, the number of legitimate transactions is significantly higher than the number of fraudulent transactions. As a result, machine learning models trained on such datasets may become biased toward the majority class and incorrectly classify most transactions as legitimate. Although such models may appear to achieve high overall accuracy, they can perform poorly in detecting actual fraudulent activities, which are the primary focus of fraud prevention systems. Appropriate data preprocessing is essential for addressing this challenge. The preprocessing stage involves cleaning incomplete or inconsistent data, removing duplicate records, handling missing values, detecting outliers, encoding categorical variables, and normalizing numerical features. Feature engineering can also help identify meaningful behavioural patterns, such as unusual transaction frequency, transaction amount, location changes, device usage, and abnormal login behaviour. These processes improve the quality of input data and enable machine learning models to distinguish more effectively between legitimate and fraudulent transactions.

Resampling techniques are widely used to address class imbalance. Oversampling methods increase the representation of minority-class fraud cases, while under sampling reduces the number of majority-class legitimate transactions. Synthetic data generation techniques, such as the Synthetic Minority Over-sampling Technique (SMOTE), can create artificial examples of fraudulent transactions based on existing minority-class patterns. Hybrid approaches combining oversampling and under sampling may also improve dataset balance while reducing the risk of information loss [14].

However, resampling techniques must be carefully applied because excessive oversampling can lead to overfitting, while excessive under sampling may remove important information from legitimate transactions. Therefore, model performance should be evaluated using appropriate metrics such as precision, recall, F1-score, Area Under the ROC Curve (AUC-ROC), and precision-recall curves rather than relying only on accuracy.
Overall, addressing highly imbalanced banking transaction datasets through effective preprocessing and resampling techniques is essential for improving fraud detection performance. A balanced and well-prepared dataset enables machine learning models to identify rare fraudulent transactions more accurately while minimizing false positives and maintaining reliable performance in real-world digital banking environments.

COMPARE MACHINE LEARNING MODELS USING ACCURACY, PRECISION, RECALL, F1-SCORE, ROC-AUC, AND FRAUD-DETECTION RATE

Evaluation Metric	Purpose in Fraud Detection
Accuracy	Measures the overall percentage of transactions correctly classified as fraudulent or legitimate.
Precision	Measures how many transactions predicted as fraudulent are actually fraudulent.
Recall	Measures how many actual fraudulent transactions are correctly identified by the model.
F1-Score	Provides a balance between precision and recall, making it useful when fraud cases are relatively rare.
ROC-AUC	Measures the model's ability to distinguish between fraudulent and legitimate transactions across different classification thresholds.
Fraud-Detection Rate	Measures the proportion of actual fraudulent transactions successfully detected by the model; it is closely related to recall.

Table 4

Objective in Tabular Form

Objective	Description
Model Comparison	**To compare Logistic Regression, Decision Tree, Random Forest, and Gradient Boosting models based on their performance.**
Evaluation Parameters	**Accuracy, precision, recall, F1-score, ROC-AUC, and fraud-detection rate will be used to evaluate each model.**
Primary Focus	**To identify the model that can detect fraudulent transactions effectively while minimizing incorrect fraud predictions.**
Expected Outcome	**To determine the most suitable machine learning model for reliable and effective fraud detection.**

Table 5

THE TRADE-OFF BETWEEN FRAUD DETECTION AND FALSE-POSITIVE RATES

An important objective of a machine learning-based fraud prevention system in digital banking is to identify and analyze the trade-off between fraud detection rates and false-positive rates. Fraud detection rate refers to the ability of a system to correctly identify genuinely fraudulent transactions, whereas the false-positive rate refers to legitimate transactions that are incorrectly classified as fraudulent. Achieving a balance between these two measures is essential for developing an effective and customer-friendly fraud prevention framework.

A highly sensitive fraud detection system may identify a greater number of suspicious transactions, thereby increasing the fraud detection rate. However, excessive sensitivity can also result in a higher number of false positives, where genuine customers experience blocked transactions, unnecessary authentication requests, or account restrictions. Such incidents may negatively affect customer satisfaction, trust, and the overall digital banking experience. Conversely, reducing the false-positive rate too aggressively may allow some fraudulent transactions to remain undetected, resulting in financial losses and security risks.

Machine learning algorithms can help address this challenge by analyzing historical transaction patterns, customer behaviour, transaction amounts, locations, devices, and other relevant features. By assigning risk scores and adjusting classification thresholds, banks can optimize the balance between detecting fraudulent activities and minimizing unnecessary disruptions to legitimate customers [16].

Therefore, evaluating performance metrics such as precision, recall, accuracy, false-positive rate, and the F1-score is necessary to assess the effectiveness of fraud detection models. This objective aims to determine the most appropriate balance between security and customer convenience. A well-optimized machine learning framework

can improve fraud detection accuracy while reducing false alarms, enabling digital banks to provide secure, efficient, and reliable financial services.

IMPLEMENTING AI-BASED FRAUD DETECTION IN BANKING AND FINTECH ENVIRONMENTS, INCLUDING SCALABILITY, EXPLAINABILITY, REAL-TIME PROCESSING, AND ADAPTABILITY

The successful implementation of AI-based fraud detection systems in banking and financial technology environments depends on several practical requirements. This objective focuses on examining the key technological and operational factors necessary to ensure that artificial intelligence systems can effectively detect and prevent fraudulent activities in real-world financial environments. Among the most important requirements are scalability, explainability, real-time processing, and adaptability.

Scalability is essential because banks and fintech companies process a large volume of transactions every second. An AI-based fraud detection system must be capable of handling increasing amounts of customer, transaction, and behavioural data without affecting system performance. Cloud computing and distributed machine learning infrastructure can support the processing of large-scale financial data efficiently [8].

Explainability is another important requirement, particularly in highly regulated financial environments. AI models should provide understandable reasons for identifying a transaction as fraudulent. Explainable AI can help fraud analysts, banking professionals, regulators, and customers understand the factors influencing automated decisions. This improves transparency, accountability, and trust in AI-based systems.

Real-time processing is also critical for proactive fraud prevention. Fraud detection systems must analyze transactions immediately and generate risk scores within a short period. Delays in identifying suspicious activities may allow fraudulent transactions to be completed before intervention occurs. Therefore, AI systems should be integrated with real-time monitoring and automated response mechanisms.

Adaptability is equally important because fraud techniques continuously evolve. Static rule-based systems may become ineffective when criminals develop new methods of attack. Machine learning models should therefore be continuously monitored, updated, and retrained using new data to identify emerging fraud patterns.

Overall, examining these practical requirements helps determine whether AI-based fraud detection systems can operate effectively in real banking and fintech environments. A successful implementation requires a balance between advanced technological capabilities, operational efficiency, regulatory compliance, data privacy, and customer convenience.

MACHINE LEARNING-BASED FRAMEWORK THAT CAN SUPPORT PROACTIVE FRAUD PREVENTION IN DIGITAL BANKING

A Machine Learning-Based Framework for proactive fraud prevention in digital banking is designed to identify, predict, and mitigate fraudulent activities before they cause significant financial losses. Unlike traditional rule-based fraud detection systems, which mainly react to predefined suspicious patterns, machine learning algorithms can continuously learn from historical and real-time transaction data to detect complex and evolving fraudulent behaviour. This approach enables banks and financial institutions to move from reactive fraud detection toward proactive fraud prevention.

The framework typically begins with the collection and integration of data from multiple sources, including transaction history, customer profiles, login behaviour, device information, geographic location, payment patterns, and digital interaction data. These datasets are then cleaned, processed, and transformed into meaningful features that can support fraud prediction. Important indicators may include unusual transaction amounts, frequent login attempts, changes in device usage, abnormal transaction locations, and deviations from a customer's normal spending behaviour [17].

Machine learning models such as Random Forest, Decision Trees, Support Vector Machines, Neural Networks, and Gradient Boosting can be used to classify transactions as legitimate or potentially fraudulent. In addition, unsupervised learning techniques such as clustering and anomaly detection are useful for identifying previously

unknown fraud patterns. Real-time analytics allows these models to evaluate transactions instantly and assign a fraud risk score based on the probability of suspicious activity.

A proactive framework can also incorporate automated response mechanisms. When a high-risk transaction is detected, the system may temporarily block the transaction, request additional authentication, notify the customer, or escalate the case for manual investigation. Continuous model monitoring and retraining are essential because fraud techniques constantly evolve and historical patterns may become outdated.

Furthermore, explainable artificial intelligence can improve transparency by helping fraud analysts understand why a particular transaction was classified as suspicious. This increases trust in automated decision-making and supports regulatory compliance. Data security and privacy must also be integrated into the framework to ensure the responsible use of sensitive customer information [15].

Overall, a machine learning-based framework provides an intelligent and adaptive approach to fraud prevention in digital banking. By combining predictive analytics, real-time monitoring, anomaly detection, and automated intervention, financial institutions can detect emerging threats earlier, reduce financial losses, enhance customer security, and build greater trust in digital banking services.

THREATS

Although Artificial Intelligence and Machine Learning provide powerful mechanisms for fraud prevention, their implementation in digital banking introduces several technical, operational, security, and ethical threats. These threats should be considered when evaluating the proposed framework.

- **Data Privacy and Confidentiality -** Digital banking fraud-detection systems require access to transaction histories, customer behaviour, device information, geographic information, and authentication-related data. Such information is highly sensitive. Unauthorized access, poor data governance, or inappropriate sharing of datasets can expose customers to privacy risks.
- Financial institutions must therefore implement appropriate encryption, access control, anonymization, data minimization, and secure data-storage mechanisms. Privacy-preserving approaches such as federated learning may also help institutions collaborate without directly sharing raw transaction data. Recent research has specifically investigated federated approaches for fraud detection because financial transaction data are often distributed across institutional data silos. (Tang & Liang, 2024).
- **Class-Imbalance Threat -** Fraudulent transactions normally represent only a small proportion of total transactions. Consequently, an ML model trained on an imbalanced dataset may become biased toward legitimate transactions. A model may report high overall accuracy while failing to detect a substantial proportion of fraud. This problem makes precision, recall, F1-score, ROC-AUC, and particularly fraud-sensitive evaluation more meaningful than accuracy alone. Research on realistic fraud detection has demonstrated that class imbalance is one of the central challenges of operational fraud-detection systems.
- **Concept Drift -** Fraudulent behaviour changes continuously. Fraudsters may modify transaction amounts, devices, locations, accounts, payment methods, and attack strategies to avoid detection. At the same time, legitimate customer behaviour also changes. This phenomenon is known as **concept drift**. A model that performs effectively on historical data may gradually lose effectiveness when deployed in a changing environment. Dal Pozzolo et al. (2018) identified concept drift, class imbalance, and verification latency as important challenges in real-world fraud detection.
- **Adversarial Attacks -** Fraudsters may deliberately manipulate transaction characteristics to avoid AI-based detection. For example, an attacker may imitate a legitimate customer's transaction amount, location, timing, or device behaviour.
- Therefore, fraud-detection models themselves may become targets of adversarial manipulation. Continuous monitoring, model validation, anomaly detection, and secure model-management procedures are required to reduce this threat.
- **False Positives -** A false positive occurs when a legitimate transaction is incorrectly classified as fraudulent. Excessive false positives can result in blocked payments, unnecessary authentication requests, customer dissatisfaction, and additional investigation costs.

- This creates a critical trade-off between **fraud detection rate and customer convenience**. A model that maximizes recall without controlling false positives may not be appropriate for practical banking applications.
- **False Negatives -** A false negative occurs when a fraudulent transaction is classified as legitimate. This represents a direct fraud-prevention failure and may cause financial losses to customers and financial institutions. Consequently, the cost of false negatives can be considerably greater than the cost of some false positives. Cost-sensitive learning and threshold optimization can therefore be incorporated into the proposed framework.
- **Explainability and Regulatory Risk -** Complex ensemble and AI models can be difficult to interpret. Banking institutions may need to explain why a transaction was classified as high risk, particularly when an account or payment is blocked. Explainable AI can improve transparency by identifying the features that contributed to a fraud prediction [16]. Recent work has also emphasized the importance of combining predictive performance with interpretability and regulatory compliance.
- **Data Leakage -** Data leakage occurs when information from the testing period or target variable unintentionally influences model training. This can produce unrealistically high evaluation results. The problem is particularly important when resampling methods such as SMOTE are used. Sampling should normally be performed only on the training data after the train-test split. Otherwise, information from synthetic or duplicated observations can leak into the test set.
- **Real-Time Processing Threat -** Digital banking systems process large numbers of transactions continuously. A fraud-detection model must therefore produce predictions with sufficiently low latency. An algorithm that is highly accurate but computationally expensive may be unsuitable for real-time transaction authorization. Therefore, scalability, inference time, memory requirements, and infrastructure costs must be evaluated alongside predictive accuracy.

DATA ANALYSIS

Q1. How effective do you consider Artificial Intelligence and Machine Learning in preventing fraud in digital banking?

Table 6.1

Opinion	Respondents	Percentage
Not effective at all	0	0
Slightly effective	0	0
Moderately effective	0	0
Highly effective	100	100
Extremely effective	0	0
Total	100	100

Table 6.2

Sample Standard Deviation, s	44.721359549996
Variance (Sample Standard), s^2	2000
Population Standard Deviation, σ	40
Variance (Population Standard), σ^2	1600
Total Numbers, N	5
Sum:	100
Mean (Average):	20
Standard Error of the Mean (SE$\bar{x}$):	20

Primary Resource

Q2. Which machine learning approach do you believe is most effective for detecting fraudulent banking transactions?

Table 7.1

Opinion	Respondents	Percentage
Logistic Regression	0	0
Decision Tree	0	0

ISSN 2349-4506
Impact Factor: 3.799
Global Journal of Engineering Science and Research Management

Random Forest	100	100
Gradient Boosting	0	0
Isolation Forest	0	0
Total	100	100

Table 7.2

Sample Standard Deviation, s	44.721359549996
Variance (Sample Standard), s^2	2000
Population Standard Deviation, σ	40
Variance (Population Standard), σ^2	1600
Total Numbers, N	5
Sum:	100
Mean (Average):	20
Standard Error of the Mean (SE$\bar{x}$):	20

Primary Resource

Q3. How important is anomaly detection in identifying unusual and potentially fraudulent banking transactions?

Table 8.1

Opinion	Respondents	Percentage
Not important	0	0
Slightly important	0	0
Moderately important	0	0
Very important	100	100
Extremely important	0	0
Total	100	100

Table 8.2

Sample Standard Deviation, s	44.721359549996
Variance (Sample Standard), s^2	2000
Population Standard Deviation, σ	40
Variance (Population Standard), σ^2	1600
Total Numbers, N	5
Sum:	100
Mean (Average):	20
Standard Error of the Mean (SE$\bar{x}$):	20

Primary Resource

Q4. Which performance measure is most important when evaluating a fraud detection model?

Table 9.1

Opinion	Respondents	Percentage
Accuracy	0	0
Precision	0	0
Recall	100	100
F1-Score	0	0
ROC-AUC	0	0
Total	100	100

Table 9.2

Sample Standard Deviation, s	44.721359549996
Variance (Sample Standard), s^2	2000

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

Population Standard Deviation, σ	40
Variance (Population Standard), σ^2	1600
Total Numbers, N	5
Sum:	100
Mean (Average):	20
Standard Error of the Mean (SE$\bar{x}$):	20

Primary Resource

Q5. What is the biggest challenge in implementing AI-based fraud detection systems in digital banking?

Table 10.1

Opinion	Respondents	Percentage
High computational cost	0	0
Imbalanced transaction datasets	100	100
High,false-positive rates	0	0
Lack of real-time processing capability	0	0
Difficulty in explaining AI decisions	0	0
Total	100	100

Table 10.2

Sample Standard Deviation, s	44.721359549996
Variance (Sample Standard), s^2	2000
Population Standard Deviation, σ	40
Variance (Population Standard), σ^2	1600
Total Numbers, N	5
Sum:	100
Mean (Average):	20
Standard Error of the Mean (SE$\bar{x}$):	20

Primary Resource

KEY FINDINGS

The study on **Artificial Intelligence-Based Fraud Detection in Digital Banking: A Comparative Machine Learning Approach** highlights the growing importance of Artificial Intelligence (AI) and Machine Learning (ML) in strengthening fraud prevention within digital banking and fintech environments. The findings demonstrate that machine learning-based approaches can support the identification of fraudulent transactions by learning patterns from historical transaction data and detecting deviations from normal customer behaviour.

Overall, the study finds that **AI and Machine Learning have substantial potential to enhance fraud detection in digital banking**, particularly when models are selected, trained, and evaluated according to the characteristics of highly imbalanced transaction data. The comparative analysis suggests that ensemble methods such as Random Forest and Gradient Boosting are strong candidates for detecting complex fraudulent patterns, while Isolation Forest provides complementary value for identifying previously unseen or unusual transactions.

The research further establishes that successful fraud detection cannot be judged solely by overall accuracy. **Recall, precision, F1-score, ROC-AUC, fraud-detection rate, and false-positive rate must be considered together** to determine whether a model is suitable for real-world banking applications. The most effective solution is therefore not necessarily the model with the highest single performance metric, but the model or combination of models that provides an appropriate balance between fraud detection, false-positive reduction, computational efficiency, explainability, and real-time applicability.

The findings ultimately support the development of a **hybrid, scalable, and adaptive AI-based fraud-detection framework** that combines supervised machine learning, anomaly detection, and ensemble learning. Such a

framework can contribute to proactive fraud prevention while supporting the operational and customer-service requirements of modern digital banking and fintech environments.

ADVANTAGE

- **Improved Fraud Detection -** AI models can analyze large numbers of transactions and identify complex relationships that are difficult to detect using manually written rules. Machine learning can therefore support more adaptive fraud prevention.
- **Detection of Complex Patterns -** Ensemble models such as Random Forest and Gradient Boosting can identify nonlinear relationships among transaction amount, transaction frequency, time, location, customer behaviour, and other variables.
- **Anomaly Detection -** Anomaly-detection techniques can identify transactions that deviate from normal behavioural patterns. This is particularly useful for detecting potentially novel fraud that has not previously been labelled in a training dataset. Research reviews identify anomaly detection as an important component of financial fraud research, especially where supervised labels are incomplete.
- **Real-Time Fraud Prevention -** AI-based systems can assign risk scores to transactions as they occur. High-risk transactions can be blocked or subjected to additional authentication, while lower-risk transactions can proceed automatically.
- **Reduction of Manual Work -** Automated fraud scoring can reduce the number of transactions requiring manual investigation. Human analysts can concentrate on complex or high-risk cases.
- **Adaptability -** Machine learning models can be periodically retrained using new transaction data. This provides greater adaptability than static rule-based systems.
- **Ensemble Robustness -** Ensemble models combine multiple learners, reducing dependence on a single classifier. Research has demonstrated the usefulness of ensemble approaches for highly imbalanced credit-card fraud datasets.
- **Scalability -** Once appropriately implemented, an automated model can evaluate large volumes of transactions without requiring proportional increases in manual staff.
- **Support for Proactive Fraud Prevention -** AI can move fraud management from a reactive approach toward proactive risk assessment by identifying suspicious behavioural patterns before significant losses occur.

DISADVANTAGE

- **High Implementation Cost -** Developing an AI-based fraud-detection system requires investment in data infrastructure, computing resources, cybersecurity, model development, monitoring, and specialized personnel.
- **Dependence on Data Quality -** Poor-quality, incomplete, outdated, or biased data can reduce model effectiveness. AI systems learn from available data; therefore, inaccurate training data can produce inaccurate predictions.
- **Class-Imbalance Problem -** The extremely small proportion of fraudulent transactions can make conventional machine learning difficult to train effectively. Sampling, class weighting, threshold optimization, or other specialized techniques may be required.
- **False Positives -** Even a high-performing model may incorrectly identify legitimate customer behaviour as fraudulent. Excessive false alerts can damage customer experience.
- **Lack of Interpretability -** Some advanced machine learning models can function as black boxes. This may make it difficult for investigators and customers to understand individual decisions.
- **Model Drift -** The performance of a fraud model may decline as fraud strategies and customer behaviour change. Continuous monitoring and retraining are therefore required.
- **Computational Requirements -** Complex ensemble or deep learning models may require substantial computational resources, particularly when processing large transaction streams in real time.
- **Security Vulnerabilities -** Attackers may attempt to manipulate transaction characteristics or exploit weaknesses in the model. Therefore, AI systems require cybersecurity controls in addition to conventional fraud controls.
- **Privacy Concerns -** The use of behavioural and transaction data creates privacy risks if data are collected, stored, processed, or shared improperly.

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

COMPARISON

The proposed research compares Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and Isolation Forest according to predictive capability, interpretability, anomaly-detection capability, and suitability for digital banking.

Model	Learning Type	Fraud Detection	Anomaly Detection	Interpretability	Imbalanced Data Handling	Real-Time Suitability
Logistic Regression	Supervised	Moderate	Low	High	Moderate with class weights	High
Decision Tree	Supervised	Moderate	Low–Moderate	High	Moderate	High
Random Forest	Supervised Ensemble	High	Moderate	Moderate	High with appropriate tuning	High
Gradient Boosting	Supervised Ensemble	Very High	Moderate	Moderate	High with appropriate tuning	Moderate–High
Isolation Forest	Unsupervised	Moderate for unknown patterns	High	Moderate	High because it does not require fraud labels	High
Hybrid Ensemble + Isolation Forest	Hybrid	Potentially Very High	Very High	Moderate	High	Moderate–High

Table 11

The comparison indicates that **Logistic Regression** is useful as a baseline because of its simplicity and interpretability. However, it may not capture complex nonlinear transaction relationships.

Decision Tree provides more flexible decision boundaries and is relatively easy to interpret, but a single tree can become unstable or overfit.

Random Forest is expected to provide stronger and more robust performance because it combines multiple decision trees. Ensemble research in credit-card fraud detection has shown the usefulness of combining different learning mechanisms to address the highly skewed distribution of legitimate and fraudulent transactions.

Gradient Boosting is expected to perform strongly because sequential tree construction allows the model to focus on previous classification errors. Modern research has also investigated XGBoost and related boosting approaches for fraud detection and imbalanced transaction datasets.

Isolation Forest differs from the supervised models because it is primarily an anomaly-detection method. Its major advantage is the ability to identify unusual observations without requiring every fraudulent transaction to be labelled. Isolation Forest was originally proposed as an efficient method for isolating anomalies in high-dimensional datasets (Liu et al., 2008).

The **hybrid model** combining supervised ensemble learning and anomaly detection is therefore particularly relevant to the research objectives. Supervised models can identify known fraud patterns, while anomaly detection can provide additional signals for previously unseen or unusual behaviour.

- **Proposed Fraud Prevention Framework**

The research proposes a multi-layer AI-based fraud prevention framework:

Digital Banking Transaction
↓
Data Collection
↓
Data Cleaning and Preprocessing
↓
Feature Engineering
↓

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

Class-Imbalance Handling
↓
Parallel AI Detection
→ Logistic Regression
→ Decision Tree
→ Random Forest
→ Gradient Boosting
→ Isolation Forest
↓
Model Ensemble and Anomaly Score
↓
Risk Score Generation
↓
Decision Engine
→ Low Risk: Approve
→ Medium Risk: Additional Authentication
→ High Risk: Block/Manual Investigation
↓
Feedback and Model Monitoring
↓
Periodic Retraining

The feedback mechanism is particularly important because fraud patterns evolve over time. Real-world fraud research has emphasized concept drift and the need for learning strategies that reflect the changing nature of transaction streams.

Artificial Intelligence-based fraud detection represents an important advancement in digital banking security. The growth of online banking, mobile payments, digital wallets, and fintech services has increased both the volume and complexity of financial transactions, making traditional static fraud-detection mechanisms increasingly insufficient for sophisticated and evolving fraud patterns.

This research proposes a comparative machine learning approach involving Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and Isolation Forest. The framework specifically addresses the major challenges of digital banking fraud detection, including class imbalance, concept drift, false positives, false negatives, anomaly detection, explainability, privacy, and real-time processing.

Among the supervised models, Logistic Regression provides a useful and interpretable baseline, while Decision Tree offers simple nonlinear decision-making. Random Forest provides the benefits of ensemble learning and is expected to offer robust performance. Gradient Boosting is capable of modelling complex relationships and may provide strong predictive performance when appropriately tuned. Isolation Forest provides a complementary capability because it can identify unusual transactions without requiring complete fraud labels.

The comparison also demonstrates that **no single performance metric is sufficient** for evaluating a banking fraud-detection system. Accuracy can be misleading when legitimate transactions greatly outnumber fraudulent transactions. Precision, recall, F1-score, ROC-AUC, fraud-detection rate, and false-positive rate should therefore be considered together.

The proposed hybrid approach, which combines supervised ensemble learning with anomaly detection, offers a promising direction for proactive fraud prevention. Supervised models can identify known fraud patterns, while anomaly detection can identify unusual or previously unseen behaviours. Such a combination may provide broader protection than relying on either technique independently.

However, successful deployment requires more than high predictive accuracy. Banks and fintech organizations must consider data privacy, model explainability, cybersecurity, computational cost, scalability, regulatory requirements, and continuous model monitoring. Concept drift also means that fraud models should be periodically evaluated and retrained rather than treated as permanent solutions.

AI-based fraud detection can provide banking institutions with a scalable and adaptive mechanism for reducing fraudulent transactions and financial losses. The proposed comparative framework can assist researchers and financial institutions in selecting appropriate machine learning techniques according to their operational requirements. Future research should extend the framework toward real-time streaming data, graph-based fraud detection, federated learning, explainable AI, and hybrid deep-learning architectures.

CONCLUSION

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful technologies for strengthening fraud prevention in digital banking and fintech environments. This study demonstrates that AI-based fraud detection can provide more proactive, adaptive, and data-driven approaches than traditional rule-based systems. The comparative evaluation of Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and Isolation Forest highlights the importance of selecting appropriate algorithms according to the characteristics of banking transaction data.

Supervised learning techniques can effectively identify known fraudulent patterns, while anomaly detection methods such as Isolation Forest provide additional capabilities for detecting unusual transactions that may not conform to previously observed fraud patterns. Ensemble learning, particularly methods that combine multiple decision-making models, can further improve detection robustness and reduce the limitations associated with individual algorithms. However, the highly imbalanced nature of fraud datasets remains a significant challenge, making preprocessing, feature engineering, and appropriate resampling essential for reliable model performance. The evaluation of models using accuracy, precision, recall, F1-score, ROC-AUC, and fraud-detection rate provides a comprehensive basis for comparison. Importantly, the study emphasizes that high accuracy alone is insufficient for banking fraud detection, as false positives can negatively affect legitimate customers and operational efficiency. Therefore, achieving an appropriate balance between fraud detection and false-positive rates is critical.

For practical deployment, AI-based fraud detection systems must also provide scalability, real-time processing, explainability, and adaptability to evolving fraud strategies. Overall, the proposed ML-based framework can support proactive fraud prevention by combining supervised classification, anomaly detection, and ensemble learning. Such an integrated approach can help banks and fintech organizations enhance transaction security, reduce financial losses, and build greater trust in digital banking services.

REFERENCES

1. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *Proceedings of the Eighth IEEE International Conference on Data Mining* (pp. 413–422). IEEE. https://doi.org/10.1109/ICDM.2008.17
2. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems, 29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643
3. Sohony, I., Pratap, R., & Nambiar, U. (2018). Ensemble learning for credit card fraud detection. In *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data* (pp. 289–294). ACM. https://doi.org/10.1145/3152494.3156815
4. Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning. In *2019 International Conference on Innovations in Information and Communication Technology (ICIICT)*. IEEE. https://doi.org/10.1109/CONFLUENCE.2019.8776942
5. Acharya, V., & others. (2020). Credit card fraud detection using machine learning algorithms. *Procedia Computer Science, 165*, 631–641. https://doi.org/10.1016/j.procs.2020.01.057
6. Al-Dhaqm, A., et al. (2020). A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. *Scientific African, 8*, e00464. https://doi.org/10.1016/j.sciaf.2020.e00464
7. Gubran Al-Hashedi, K., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review, 40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402
8. 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. https://doi.org/10.3390/app12199637

ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

9. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429
10. Yi, Z., Cao, X., Pu, X., Wu, Y., Chen, Z., Khan, A. T., Francis, A., & Li, S. (2023). Fraud detection in capital markets: A novel machine learning approach. *Expert Systems with Applications, 231*, 120760. https://doi.org/10.1016/j.eswa.2023.120760
11. Tang, Y., & Liang, Y. (2024). Credit card fraud detection based on federated graph learning. *Expert Systems with Applications, 256*, 124979. https://doi.org/10.1016/j.eswa.2024.124979
12. Ahmed, K. H., Axelsson, S., Li, Y., & Sagheer, A. M. (2025). A credit card fraud detection approach based on ensemble machine learning classifier with hybrid data sampling. *Machine Learning with Applications, 20*, 100675. https://doi.org/10.1016/j.mlwa.2025.100675
13. Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., et al. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12*, 6. https://doi.org/10.1186/s40537-024-01048-8
14. Shih, Y.-C., Dai, T.-S., Chen, Y.-P., Ti, Y.-W., Wang, W.-H., & Kuo, Y. (2025). Fund transfer fraud detection: Analyzing irregular transactions and customer relationships with self-attention and graph neural networks. *Expert Systems with Applications, 259*, 125211. https://doi.org/10.1016/j.eswa.2024.125211
15. Al-Bulushi, A., Shaikh, A. K., & Adhikari, N. (2026). Applying supervised machine learning algorithms and ensemble models to enhance credit card fraud detection. *Frontiers in Artificial Intelligence, 9*, 1813728. https://doi.org/10.3389/frai.2026.1813728
16. A Study on Comparative analysis of AI regulation in the EU, US, and China. (2026). *International Journal of Artificial Intelligence, Machine Learning and Data Analytics, 1*(1), 1-12. https://doi.org/10.68033/ijaimda.1.1.1-12
17. Hamdulay N. A.,(2026). Prompt Engineering as Rhetorical Practice: Redefining Literacy in AI-Mediated Education. International Journal of Education, Society and Policy, 1(1), 50-59.https://ijesp.org/index.php/ijesp/article/view/18 DOI: https://doi.org/10.64149/m1m0x339
18. Khoozani, Z. S., Seera, M., & Lim, C. P. (2026). Towards transparent financial AI: A systematic review of graph learning and explainable methods for credit risk and fraud detection. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-026-11645-z
19. Thivaios, S., Kostopoulos, G., Stefani, A., & Kotsiantis, S. (2026). A survey of machine learning and deep learning for financial fraud detection: Architectures, data modalities, and real-world deployment challenges. *Algorithms, 19*(5), 354. https://doi.org/10.3390/a19050354