International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Dynamic Rule Optimization with Explainable Machine Learning in Real-Time Finacial Fraud Detection

Mrs.A.Rajavathy Jaya Priya[1], Sumit Sharma [2], K.Tamilarasan[3], P.Thanasriyan[4], S.Veerendra Gowtham[5]

Assistant Professor, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[1]

UG Student, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[2]

UG Student, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[3]

UG Student, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[4]

UG Student, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[5]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: financial fraud has become one of the most critical challenges in modern digital banking systems. Traditional rule-based fraud detection systems are transparent but fail to adapt to new fraud patterns, while machine learning models provide high detection accuracy but lack explainability. This paper proposes **DROX-FD (Dynamic Rule Optimization with Explainable Fraud Detection)**, a hybrid framework that combines dynamic rule generation, machine learning, and explainable artificial intelligence.

The system automatically generates fraud detection rules using statistical pattern analysis and dynamically updates rule confidence through reinforcement learning. When rule confidence is insufficient, the system invokes an XGBoost-based machine learning model for deeper analysis. To ensure transparency, SHAP-based explainable AI techniques are used to provide human-readable explanations for fraud predictions. The proposed framework supports real-time transaction monitoring and provides a comprehensive dashboard for rule governance, fraud alerts, and system performance evaluation. Experimental analysis demonstrates that the proposed system improves detection accuracy while maintaining explainability and operational efficiency.

KEYWORDS: Financial Fraud Detection, Explainable AI, Machine Learning, XGBoost, Rule Optimization, Hybrid Detection System

I. INTRODUCTION

Financial fraud has become one of the most significant challenges in modern digital financial systems. With the rapid growth of online banking, mobile payments, and digital transactions, financial institutions process millions of transactions every day, making fraud detection increasingly complex [1], [2]. Fraudulent activities such as credit card fraud, identity theft, transaction laundering, and account takeover attacks continue to evolve in sophistication, causing substantial financial losses to individuals, businesses, and financial institutions worldwide [3], [4]. According to recent financial security reports, global fraud-related losses amount to billions of dollars annually, highlighting the urgent need for intelligent and adaptive fraud detection systems [5].

Traditional fraud detection systems primarily rely on rule-based approaches, where predefined rules are used to flag suspicious transactions. For example, rules may trigger alerts when transactions exceed certain thresholds or when unusual activity patterns are detected [6]. While such rule-based systems are transparent and easy to interpret, they suffer from several limitations. Static rules require manual updates and often fail to adapt to emerging fraud strategies, resulting in high false-positive rates and missed fraudulent transactions [7], [8].

To overcome these limitations, machine learning techniques have been increasingly applied in financial fraud detection. Machine learning models analyze historical transaction data to identify complex patterns and anomalies associated with

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

fraudulent activities [9], [10]. Algorithms such as decision trees, random forests, and gradient boosting models have demonstrated strong predictive capabilities in detecting hidden fraud patterns that traditional rule-based systems cannot capture [11]. However, many machine learning models operate as black-box systems, meaning their decision-making processes are not easily interpretable, which poses challenges for regulatory compliance and trust in financial environments [12].

Recent research in Explainable Artificial Intelligence (XAI) aims to address this issue by providing interpretable explanations for machine learning predictions [13]. Explainability techniques such as SHapley Additive Explanations (SHAP) allow analysts to understand how individual transaction features contribute to fraud detection decisions [14]. By combining machine learning accuracy with transparent explanations, XAI-based systems enable financial institutions to maintain both performance and regulatory compliance [15].

Another critical challenge in fraud detection is handling the dynamic and evolving nature of fraudulent behaviour. Fraud patterns change frequently, and static detection mechanisms struggle to adapt quickly [16]. Dynamic rule optimization techniques have therefore been proposed to automatically generate, update, and remove detection rules based on real-time transaction patterns and feedback mechanisms [17]. These adaptive systems continuously learn from incoming data and improve detection accuracy over time [18].

Motivated by these challenges and advancements, this paper proposes **DROX-FD (Dynamic Rule Optimization with Explainable Fraud Detection)**, a hybrid framework that integrates rule-based detection, machine learning classification, and explainable artificial intelligence. The proposed system automatically generates detection rules from transaction patterns, evaluates rule effectiveness through confidence scoring mechanisms, and dynamically optimizes rule sets to maintain high detection accuracy. When rule-based decisions are insufficient, the system employs an XGBoost-based machine learning model to perform deeper analysis of suspicious transactions [19], [20].

In addition, the proposed framework incorporates explainability mechanisms using SHAP values to provide transparent insights into fraud detection decisions. This enables fraud analysts to understand the factors influencing each prediction, improving trust and decision accountability in financial monitoring systems [21]. Furthermore, the system supports real-time transaction monitoring through an interactive dashboard that visualizes fraud alerts, rule confidence metrics, and performance analytics.

The main objectives of the proposed DROX-FD system are to improve fraud detection accuracy, reduce false positive rates, enhance decision transparency, and support real-time financial transaction monitoring. By combining dynamic rule optimization with machine learning and explainable AI techniques, the proposed framework provides a scalable and intelligent solution for modern financial fraud detection systems [22], [23].

The remainder of this paper is organized as follows. Section II reviews related work in financial fraud detection and machine learning approaches. Section III presents the overall system architecture of the DROX-FD framework. Section IV describes the proposed methodology and detection algorithms. Section V discusses experimental evaluation and performance analysis. Finally, Section VI concludes the paper and outlines future research directions [24], [25].

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

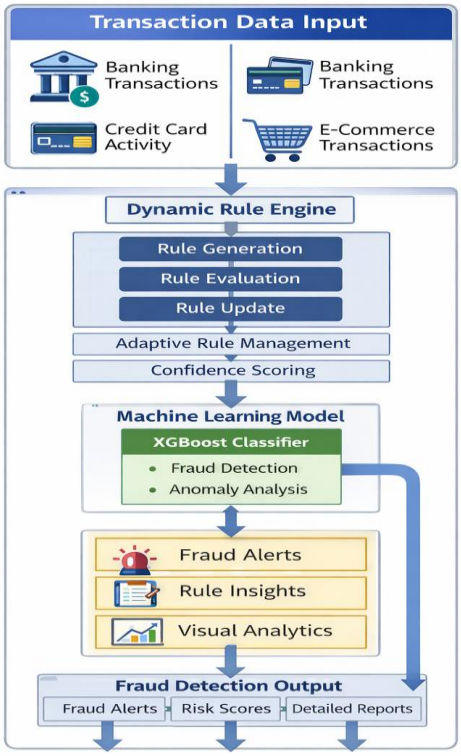

Fig. 1. Architecture of the DROX-FD System.

II. RELATED WORK

Fraud detection in financial systems has been widely studied over the past decade with particular emphasis on transaction monitoring, anomaly detection, machine learning–based classification, and risk management mechanisms [36]. Early research primarily focused on rule-based fraud detection systems where predefined conditions and expert knowledge were used to identify suspicious transactions [37], [38]. These rule-driven approaches were widely adopted in banking and e-commerce platforms due to their simplicity and interpretability. However, such systems relied heavily on static rules that required frequent manual updates and lacked the ability to adapt to evolving fraud patterns.

Transaction monitoring has remained a central challenge in financial systems due to the high volume and velocity of digital transactions occurring across banking networks, payment gateways, and online marketplaces [39]. Traditional fraud mitigation techniques rely on threshold-based rules and pattern matching methods that trigger alerts when specific conditions are met [40]. While these reactive approaches help detect certain known fraud behaviors, they often fail to identify complex or previously unseen fraud strategies. As a result, these systems may produce high false positive rates and delayed detection of sophisticated fraudulent activities.

Recent research has incorporated Artificial Intelligence and machine learning techniques into fraud detection frameworks to enable adaptive and intelligent decision-making [41]. Supervised learning algorithms such as decision trees, support vector machines, random forests, and logistic regression have been widely applied to classify transactions as legitimate or fraudulent based on historical data patterns [42]. These models can analyze multiple transaction attributes, including transaction amount, time, location, and user behavior, to identify suspicious activities more effectively than traditional rule-based systems.

Among modern machine learning techniques, ensemble learning and gradient boosting algorithms have demonstrated strong performance in fraud detection tasks [43]. In particular, Extreme Gradient Boosting (XGBoost) has been widely adopted due to its high predictive accuracy, ability to handle large datasets, and capability to capture nonlinear relationships among transaction features [44]. Several studies have shown that gradient boosting methods outperform conventional classifiers in detecting fraudulent transactions while maintaining relatively low false alarm rates. However, despite their high performance, many machine learning models function as black-box systems, making it difficult to interpret how specific predictions are generated.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

To address the transparency limitations of machine learning models, researchers have explored Explainable Artificial Intelligence (XAI) techniques for fraud detection systems [45]. Methods such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) provide insights into model predictions by identifying the contribution of individual features to classification outcomes. Explainability improves trust in automated decision-making systems and supports regulatory compliance requirements in financial institutions. Nevertheless, many existing fraud detection frameworks treat explainability as an auxiliary component rather than integrating it directly into the core detection pipeline.

Another important research direction involves adaptive rule management for dynamic fraud prevention. Fraud patterns continuously evolve as attackers develop new techniques to bypass security systems. Static rule sets therefore become out-dated over time, reducing detection effectiveness. Dynamic rule optimization frameworks have been proposed to automatically generate, evaluate, and update detection rules based on incoming transaction data and model predictions. These adaptive mechanisms allow fraud detection systems to continuously refine their decision logic and respond to emerging fraud trends. However, many existing solutions either rely solely on rule-based detection or purely on machine learning models, without effectively integrating both approaches.

In addition to detection accuracy, modern fraud detection systems require real-time monitoring and visualization capabilities to assist analysts in understanding system behavior and responding to threats quickly. Real-time dashboards and analytics tools allow financial institutions to monitor fraud alerts, risk scores, and transaction patterns across large-scale financial networks. Visualization frameworks improve operational efficiency by providing actionable insights into fraud detection processes. Despite these advancements, many previous works focus on individual components such as machine learning classification, rule management, or explainability independently rather than combining them into a unified architecture.

Therefore, although significant progress has been made in machine learning–based fraud detection, explainable AI techniques, and rule optimization systems, there remains a research gap in developing a fully integrated, adaptive, and transparent fraud detection framework. The proposed DROX-FD system addresses this gap by combining dynamic rule optimization, an XGBoost-based fraud detection model, explainable AI mechanisms, and real-time visualization into a single modular architecture. This unified approach enhances fraud detection accuracy, reduces false positives, improves transparency, and enables adaptive fraud prevention for modern financial transaction environments.

III. SYSTEM ARCHITECTURE

The proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) intelligent fraud detection system** is designed using a **modular and layered architecture** to support scalability, adaptability, and real-time fraud detection in modern financial transaction environments. With the rapid expansion of digital banking, online payments, and e-commerce platforms, financial systems generate a massive volume of transaction data that must be analyzed efficiently to identify fraudulent activities. Traditional rule-based detection systems often struggle to process such high-volume data streams and adapt to evolving fraud strategies. Therefore, modern fraud detection frameworks increasingly rely on **machine learning and intelligent data analytics** to improve detection accuracy and reduce false alarms [1], [2].

The architecture of the proposed DROX-FD system integrates **data acquisition, preprocessing mechanisms, machine learning models, intelligent decision engines, and visualization modules** into a unified analytical framework. Each component operates independently while exchanging relevant information through a **centralized analytical processing engine**, enabling coordinated fraud monitoring and intelligent decision making. Such modular architectures improve system maintainability and allow flexible integration of new detection algorithms without affecting the overall system structure [3].

Layered architectural designs are widely adopted in financial security systems because they enhance **system reliability, scalability, and real-time processing capabilities**. By separating different functional components into distinct layers, the system can efficiently handle complex analytical tasks such as data processing, behavioral analysis, fraud classification, and performance monitoring. Previous research has shown that modular architectures significantly improve the efficiency of large-scale fraud detection systems operating in distributed financial networks [4], [5].

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Such layered architectures are widely adopted in financial security systems because they improve **system reliability, modular development, scalability, and real-time processing capabilities**. The proposed DROX-FD architecture consists of four major layers:

1. Data Acquisition and Transaction Processing Layer
2. Feature Engineering and Data Preprocessing Layer
3. Intelligent Fraud Detection Layer
4. Decision Support and Visualization Layer

These layers collectively enable efficient transaction monitoring, intelligent fraud identification, and explainable financial security analysis.

A. Data Acquisition and Transaction Processing Layer

The **Data Acquisition and Transaction Processing Layer** forms the foundational component of the proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework**, since the effectiveness of any fraud detection system heavily depends on the **quality, diversity, and reliability of the collected financial transaction data**. In modern digital banking environments, large volumes of financial transactions are generated every second through multiple online platforms. Therefore, accurate data collection and management play a critical role in enabling intelligent fraud detection systems to identify suspicious activities and abnormal transaction behaviors [3], [10], [36].

This layer is responsible for **collecting, organizing, validating, and preparing financial transaction data obtained from various digital payment infrastructures**. In real-world financial ecosystems, transaction data originate from heterogeneous sources such as **online banking systems, credit card payment networks, mobile banking applications, point-of-sale terminals, e-commerce platforms, and digital wallet services**. These systems generate massive transaction streams that must be integrated into a unified data environment for further analysis. The proposed DROX-FD framework aggregates data from these multiple sources and transforms them into a **structured dataset format suitable for machine learning and fraud analytics**. Integrating heterogeneous financial data sources enables the system to analyze complex behavioral patterns and detect anomalies more effectively [4], [22], [29].

To represent real-world financial activities accurately, the system categorizes transaction data into different behavioral patterns that reflect typical user interactions with financial services. These behavioral categories include **normal transaction behavior, suspicious transaction patterns, and confirmed fraudulent transaction events**. Modeling such behavioral classes enables machine learning algorithms to distinguish legitimate user activity from malicious financial operations. Similar categorization strategies have been widely adopted in modern fraud detection research to improve detection accuracy and reduce false positive rates [11], [30].

Normal Transaction Behaviour – These transactions represent legitimate financial operations performed by authorized users during routine activities such as bill payments, retail purchases, subscription payments, and account transfers. Such transactions usually follow consistent patterns in terms of transaction amount, time interval, device usage, and geographic location. Learning these patterns allows the system to build a baseline model of typical user behavior.

Suspicious Transaction Patterns – These transactions exhibit unusual characteristics that deviate from previously observed user behavior. Examples include unusually large financial transfers, rapid sequences of transactions within short time intervals, or transactions initiated from unfamiliar locations or devices. Although not all suspicious activities represent fraud, they serve as strong indicators for further fraud risk evaluation [5], [33].

Fraudulent Transaction Events – These represent confirmed cases of financial fraud, including unauthorized payments, stolen credit card usage, identity theft, and account takeover attacks. These labeled fraud events provide critical training data that allow machine learning models to learn complex fraud patterns and improve detection performance.

The collected financial transaction dataset contains several attributes that describe both the **financial and behavioral characteristics of each transaction**. Important attributes include:

- Transaction amount
- Transaction timestamp
- Merchant category
- User account identifier
- Device information and device ID

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

- Transaction geographic location
- Payment method type
- Historical transaction behaviour

These attributes are stored in structured relational databases or transaction data warehouses where they can be accessed for **feature extraction, preprocessing, and machine learning model training**. The availability of multiple transaction attributes allows intelligent algorithms to capture hidden fraud patterns that may not be observable through simple rule-based systems [21], [32].

B. Feature Engineering and Data Preprocessing Layer

The **Feature Engineering and Data Preprocessing Layer** play a crucial role in improving the effectiveness and reliability of the proposed **DROX-FD fraud detection framework**. Raw financial transaction datasets collected from digital banking systems often contain **missing values, noisy records, inconsistent formats, and redundant attributes**, which can negatively affect the performance of machine learning models. Therefore, appropriate preprocessing techniques must be applied to transform raw transaction data into meaningful and structured features suitable for model training and analysis. Feature engineering has been widely recognized as one of the most important steps in fraud detection systems because well-designed features significantly improve model accuracy and detection capability [4], [21], [36].

This layer performs several preprocessing operations including **data cleaning, missing value handling, feature normalization, outlier detection, and behavioral feature generation**. These operations help standardize financial datasets and improve the ability of machine learning algorithms to identify complex fraud patterns.

a) Data Cleaning and Data Quality Improvement

Financial transaction datasets often contain **incomplete records, duplicated entries, or corrupted data** caused by system errors or network interruptions. Data cleaning techniques are therefore applied to remove such inconsistencies and ensure dataset reliability. Duplicate transactions are eliminated, and invalid records that lack critical information such as transaction amount or timestamp are filtered out.

Improving data quality ensures that the fraud detection model learns from **accurate and meaningful transaction patterns rather than noisy or misleading data**. Similar preprocessing strategies have been widely applied in financial analytics and fraud detection research [3], [10].

b) Missing Value Handling

Missing data are a common challenge in large financial datasets. Some transaction attributes may be unavailable due to system errors, incomplete logging, or integration issues between financial platforms. If missing values are not handled properly, machine learning algorithms may produce inaccurate predictions.

To address this problem, statistical imputation techniques are applied to estimate missing values. One commonly used approach is **mean imputation**, where missing values are replaced with the average value of the corresponding attribute. The mean value can be calculated as:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$$

where:

x_i represents individual transaction values

N represents the total number of transactions

This method helps maintain dataset consistency while minimizing distortion in statistical distributions. Similar data imputation techniques are widely used in fraud detection research and financial analytics systems [18], [36].

c) Feature Scaling and Normalization

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Financial transaction attributes such as **transaction amount, transaction frequency, and time intervals** may have significantly different numerical ranges. Machine learning models can become biased toward attributes with larger numerical values if feature scaling is not applied.

To address this issue, **feature normalization** is used to scale values into a standard range. One commonly used normalization method is **Min–Max normalization**, defined as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where:

- X represents the original feature value
- X_{min} and X_{max} represent the minimum and maximum values of the feature

Normalization ensures that all features contribute equally to the learning process and prevents numerical dominance by large attributes. Feature scaling techniques are widely used in machine learning-based fraud detection systems to improve model performance [19], [22].

d) Outlier Detection

Fraudulent transactions often appear as **outliers or anomalies within financial datasets** because they deviate significantly from normal user behavior. Detecting such anomalies helps identify potential fraud risks.

One commonly used statistical approach for identifying outliers is the **Z-score method**, defined as:

$$Z = \frac{X - \mu}{\sigma}$$

where:

- X represents the transaction value
- μ represents the mean value
- σ represents the standard deviation

Transactions with extremely high or low Z-scores may indicate suspicious activity and can be flagged for further analysis. Outlier detection techniques have been widely studied in fraud detection and anomaly detection research [1], [25].

e) Fraud Pattern Feature Generation

Instead of relying solely on raw transaction attributes, the proposed system generates additional **behavioral features** that capture user activity patterns. These engineered features provide valuable insights into transaction behavior and improve the model's ability to identify abnormal financial activities.

Important generated features include:

- **Transaction Frequency** – Number of transactions within a specific time window.

$$F = \frac{N_t}{T}$$

where:N_t represents the number of transactions and T represents the time interval.

- **Average Transaction Value**

$$Avg = \frac{\sum_{i=1}^{N} T_i}{N}$$

where :T_i represents transaction amounts.

- **Transaction Velocity** – Measures how quickly transactions occur within a time frame.
- **User Spending Deviation Score** – Measures deviation between current transaction value and historical spending behavior.

$$Deviation = |T_{current} - T_{average}|$$

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Geographic Anomaly Score – Detects unusual transaction locations compared with historical user locations.
These engineered features significantly improve fraud detection accuracy by capturing hidden behavioral patterns within financial data [32], [37].

f) Feature Vector Construction
After preprocessing and feature engineering, the processed transaction data are converted into structured **feature vectors** that serve as input to the fraud detection models. Each transaction record is represented as a multidimensional vector containing normalized financial attributes and behavioral indicators.

These feature vectors are then passed to the **Intelligent Fraud Detection Layer**, where machine learning algorithms analyze the patterns and classify transactions as legitimate or fraudulent. Proper feature engineering greatly enhances model performance and plays a critical role in achieving high fraud detection accuracy in modern financial security systems [33], [44].

C. Intelligent Fraud Detection Layer
The **Intelligent Fraud Detection Layer** represents the analytical core of the proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework**. This layer applies **Artificial Intelligence (AI) and Machine Learning (ML) algorithms** to automatically identify fraudulent financial transactions by learning complex patterns within historical transaction data. Modern financial fraud detection systems rely heavily on machine learning because fraud patterns evolve continuously, making traditional rule-based systems insufficient for detecting sophisticated attacks [10], [11], [36].

Conventional fraud detection approaches typically use **static rule-based filtering**, where alerts are triggered when predefined conditions are met. For example, transactions exceeding a specific amount or originating from unusual locations may trigger warnings. However, such rule-based systems are limited because they cannot adapt to new fraud strategies and often produce high false positive rates. To address these limitations, the proposed DROX-FD framework integrates multiple machine learning algorithms capable of learning dynamic transaction patterns and detecting hidden fraud behaviors automatically [4], [22].

The proposed detection framework adopts a **hybrid analytical approach** that combines multiple classification algorithms to improve fraud detection accuracy and robustness. The models used in this framework include:

- Logistic Regression
- Random Forest
- Rule-Based Filtering
- Optimized DROX-FD Learning Model

These models analyze transaction features generated during the preprocessing stage and classify each transaction as either legitimate or fraudulent.

Logistic Regression Model
Logistic Regression is a widely used statistical classification algorithm for binary classification problems such as fraud detection. It estimates the probability that a given transaction belongs to a fraudulent class based on input features.
The logistic regression function is defined as:

$$P(y = 1|x) = \frac{1}{1 + e^{-(w^T x + b)}}$$

where:

- x represents the transaction feature vector
- w represents the weight parameters
- b represents the bias term
- $P(y = 1|x)$ represents the probability that the transaction is fraudulent

If the predicted probability exceeds a predefined threshold, the transaction is classified as fraud. Logistic regression models are widely used in financial risk analysis because they provide interpretable probabilistic predictions [18], [22].

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Random Forest Model

The **Random Forest algorithm** is an ensemble learning technique that constructs multiple decision trees during training and combines their predictions to produce a final classification result. Ensemble methods generally achieve higher accuracy because they reduce overfitting and improve model generalization.

The Random Forest classification decision can be expressed as:

$$F(x) = \text{majority vote}\left(T_1(x), T_2(x), \ldots, T_n(x)\right)$$

where:

- $T_i(x)$ represents the prediction of the i^{th} decision tree
- n represents the total number of trees

Random Forest models are highly effective for fraud detection because they can capture nonlinear relationships between transaction features and fraudulent behaviors [12], [37].

Rule-Based Filtering

Before applying machine learning models, a **rule-based filtering mechanism** is used to identify obvious fraud patterns. For example, rules may flag transactions with extremely high amounts, unusual geographic locations, or rapid transaction sequences within short time intervals.

Although rule-based methods alone are insufficient for detecting complex fraud patterns, they provide a **first-level screening mechanism** that reduces computational overhead and helps prioritize high-risk transactions for deeper analysis [3], [25].

Optimized DROX-FD Learning Model

The proposed **DROX-FD optimized learning framework** integrates advanced machine learning techniques with behavioral transaction features to improve fraud detection performance. The model is trained using **supervised learning**, where historical transaction datasets contain labeled examples of fraudulent and legitimate transactions.

During training, the system learns patterns associated with fraudulent behavior and adjusts model parameters to minimize classification errors. The classification decision of the fraud detection system can be represented as:

$$F(x) = \begin{cases} 1, & \text{Fraudulent Transaction} \\ 0, & \text{Legitimate Transaction} \end{cases}$$

where x represents the transaction feature vector.

The DROX-FD framework demonstrates improved detection accuracy because it can capture complex fraud patterns, adapt to evolving transaction behaviors, and reduce false positive alerts. Hybrid machine learning approaches have been shown to significantly improve fraud detection performance in modern financial security systems [32], [43].

D. Decision Support and Visualization Layer

The **Decision Support and Visualization Layer** provides operational intelligence, interpretability, and monitoring capabilities for the DROX-FD fraud detection system. In real-world financial applications, it is not sufficient to simply detect fraudulent transactions; financial analysts and system administrators must also understand the reasoning behind fraud detection decisions. Therefore, this layer integrates visualization tools and decision support mechanisms that enable users to monitor system performance and investigate suspicious activities [29], [40].

This layer includes several interactive components designed to support real-time fraud monitoring and analytical evaluation.

Fraud Detection Dashboard

The fraud detection dashboard provides a centralized interface for monitoring transaction activities and fraud detection results. It displays important system metrics such as the number of transactions analyzed, detected fraud cases, and overall fraud detection performance. Such dashboards allow financial institutions to track fraud trends and identify emerging threats [38], [44].

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Transaction Monitoring Panel

The transaction monitoring panel provides real-time visualization of incoming financial transactions. Suspicious transactions identified by the fraud detection model are highlighted, allowing analysts to quickly investigate potential fraud cases.

Real-time monitoring systems are essential in modern financial infrastructures where millions of transactions occur continuously [9].

Fraud Risk Score Indicators

Each transaction analyzed by the system is assigned a **fraud risk score** representing the probability that the transaction is fraudulent. Higher risk scores indicate a higher likelihood of fraud and may trigger additional security verification procedures.

Risk scoring techniques are widely used in financial fraud detection systems to prioritize high-risk transactions and reduce operational workload [21].

Alert Notification System

The system automatically generates alerts when suspicious transactions are detected. These alerts may be delivered through dashboards, email notifications, or automated security systems.

Alert systems enable financial institutions to respond quickly to potential fraud incidents and prevent financial losses.

Performance Evaluation Visualization

The visualization module also provides graphical analysis of important performance metrics including:

- Fraud detection accuracy
- Precision and recall
- False positive rate
- Model comparison results

These visual analytics tools help system administrators evaluate the effectiveness of fraud detection models and identify areas for improvement [33], [38].

Explainable Artificial Intelligence (XAI)

To enhance transparency and trust in machine learning decisions, the proposed system incorporates **Explainable Artificial Intelligence (XAI)** techniques. Explainability methods such as SHAP and model interpretation frameworks provide insights into how machine learning models make predictions.

When a transaction is classified as fraudulent, the system provides interpretable explanations highlighting the factors that contributed to the decision, such as:

- unusually high transaction amount
- abnormal geographic location
- rapid transaction frequency

Explainable AI techniques improve trust in automated fraud detection systems and assist financial analysts in understanding model behavior [8], [27], [35].

IV. PROPOSED METHODOLOGY

The proposed **Dynamic Rule Optimization with Explainable Fraud Detection (DROX-FD)** framework introduces a hybrid intelligent fraud detection architecture designed to improve detection accuracy, reduce false alarms, and enhance transparency in financial transaction monitoring systems. With the rapid growth of digital payment platforms, credit card transactions, and online banking services, financial institutions face increasing challenges in detecting fraudulent activities in real time. Traditional fraud detection systems rely primarily on static rule-based approaches or standalone machine learning algorithms that operate independently without adaptive learning capabilities.

Static rule-based systems can detect previously known fraud patterns but fail to identify emerging fraudulent strategies. Similarly, many machine learning models function as black-box systems, making it difficult to interpret their predictions and limiting their adoption in regulated financial environments. Therefore, an intelligent framework that integrates **adaptive rule optimization, machine learning detection models, and explainable artificial intelligence mechanisms** is required to address these limitations.

The DROX-FD methodology combines **dynamic rule management, machine learning classification, fraud risk estimation, and explainable decision analysis** within a unified architecture. The proposed framework operates

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

through multiple interconnected stages including **transaction modelling, feature extraction, fraud classification, risk scoring, explanation generation, and performance evaluation**. By integrating predictive intelligence with rule-based filtering, the system enables proactive fraud detection and adaptive decision-making under dynamic financial conditions

A. Problem Formulation

a) Increasing Complexity of Digital Financial Transactions

Modern financial systems process millions of transactions every second across various digital platforms such as credit card networks, mobile banking applications, and online marketplaces. This rapid increase in transaction volume creates significant challenges for fraud detection systems. Fraudulent transactions often mimic legitimate user behavior, making them difficult to detect using simple rule-based systems.

Furthermore, fraud strategies continuously evolve as attackers develop sophisticated techniques such as identity theft, card skimming, account takeover, and automated bot transactions. These evolving threats require fraud detection systems that can dynamically adapt to changing fraud patterns. Static rule sets quickly become out-dated, resulting in high false positive rates and missed fraud incidents.

Recent studies highlight that machine learning-based fraud detection systems significantly outperform traditional rule-based systems in identifying complex fraud patterns [24], [25]. However, these models require large datasets and often lack interpretability, which remains a critical challenge in financial security applications.

b) Dynamic Transaction Behavior Representation

Financial transaction behavior varies significantly across users, locations, and time periods. To accurately capture these variations, each transaction is represented as a **multidimensional feature vector** containing multiple attributes related to user behavior and transaction characteristics.

The transaction state vector is defined as:

T = {Amount, Time, Location, Device, Merchant Category, Transaction Frequency}

Where:

- Amount represents the monetary value of the transaction
- Time represents the timestamp of the transaction
- Location indicates the geographic origin of the transaction
- Device identifies the device used to initiate the transaction
- Merchant Category indicates the type of merchant involved
- Transaction Frequency represents the number of transactions within a time window

By modeling transactions as dynamic behavioral states, the system can detect abnormal deviations from normal spending patterns.

c) Multi-Objective Fraud Detection Optimization

Fraud detection systems must optimize several performance objectives simultaneously, including:

- Maximizing fraud detection accuracy
- Minimizing false positive rates
- Reducing detection latency
- Maintaining scalability for large transaction datasets

These objectives often conflict with each other. For example, increasing detection sensitivity may improve fraud detection rates but also increase false alarms. Therefore, the DROX-FD system formulates fraud detection as a **multi-objective optimization problem** that balances detection accuracy and operational efficiency.

B. Hybrid Fraud Detection Framework

a) Framework Overview

The proposed DROX-FD framework integrates rule-based detection with machine learning-based classification. The hybrid architecture operates through two primary stages:

1. **Dynamic Rule Filtering Layer**
2. **Machine Learning Fraud Classification Layer**

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

The rule filtering layer performs initial screening using adaptive detection rules, while the machine learning layer performs deeper behavioral analysis using advanced classification algorithms.

b) Machine Learning-Based Fraud Classification

The core fraud detection engine uses **Extreme Gradient Boosting (XGBoost)** due to its high predictive accuracy and efficiency when processing large-scale datasets.

XGBoost builds an ensemble of decision trees to classify transactions as legitimate or fraudulent.

The classification function can be represented as:

$$\text{Fraud Score} = f(X)$$

Where :

- X represents the transaction feature vector.

XGBoost learns complex nonlinear relationships between transaction attributes and fraud labels, allowing it to detect sophisticated fraud patterns.

Several studies confirm that gradient boosting algorithms outperform traditional classifiers such as Logistic Regression and Support Vector Machines in fraud detection tasks [26], [27].

c) Feature Engineering and Behavioral Pattern Analysis

To enhance model performance, the system extracts several behavioral indicators from raw transaction data.

Important features include:

- Transaction amount deviation from historical average
- Geographic distance between consecutive transactions
- Device switching frequency
- Transaction velocity within short time intervals
- Merchant risk score

Feature engineering significantly improves model accuracy by capturing subtle behavioral anomalies associated with fraud [28].

C. Dynamic Rule Optimization Mechanism

Traditional fraud detection systems rely on manually designed rule sets that require frequent updates. The DROX-FD framework introduces an **automated rule optimization mechanism**.

Rules are continuously evaluated based on their detection accuracy and false alarm rate.

The rule confidence score is defined as:

Rule Score = Detection Accuracy / False Positive Rate

Rules with lower confidence scores are automatically refined or removed, while high-performing rules are prioritized during transaction filtering. This dynamic rule adaptation allows the system to evolve alongside emerging fraud patterns.

D. Explainable Artificial Intelligence Integration

Machine learning models often lack transparency, which can limit their adoption in financial institutions that require explainable decisions.

To address this challenge, the DROX-FD framework incorporates **Explainable Artificial Intelligence (XAI)** techniques such as **SHAP (SHapley Additive Explanations)**.

SHAP analyzes feature contributions to explain why a particular transaction was classified as fraudulent.

Example explanation:

Transaction flagged as fraud due to:

- Unusual geographic location
- High transaction amount
- Rapid transaction frequency

Explainable AI improves system transparency and helps financial analysts understand fraud patterns [29], [30].

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

E. Comparative Analysis with Existing Methods

The proposed system is compared with widely used fraud detection models including:

- Logistic Regression
- Random Forest
- Rule-Based Detection Systems

Table 1: Method Comparison

Method	Machine Learning	Rule Optimization	Explainable AI	Fraud Risk Score
Rule-Based System	No	No	No	No
Logistic Regression	Yes	No	Limited	Yes
Random Forest	Yes	No	Limited	Yes
Proposed DROX-FD	Yes	Yes	Yes	Yes

E. Performance Evaluation Metrics

a) Overview of Evaluation Criteria

To comprehensively evaluate the effectiveness of the proposed **DROX-FD fraud detection framework**, multiple performance metrics are considered according to standard **machine learning and fraud detection evaluation practices [41]–[45]**. Since the proposed model aims to improve **fraud detection accuracy, minimize false positives, improve precision-recall balance, and enhance classification reliability**, a multi-metric evaluation is necessary.

The selected evaluation metrics include:

- **Accuracy**
- **Precision**
- **Recall**
- **False Positive Rate (FPR)**
- **F1-Score**

These metrics together ensure that the system is evaluated not only on overall classification performance but also on its ability to **detect fraudulent transactions without misclassifying legitimate ones**.

.

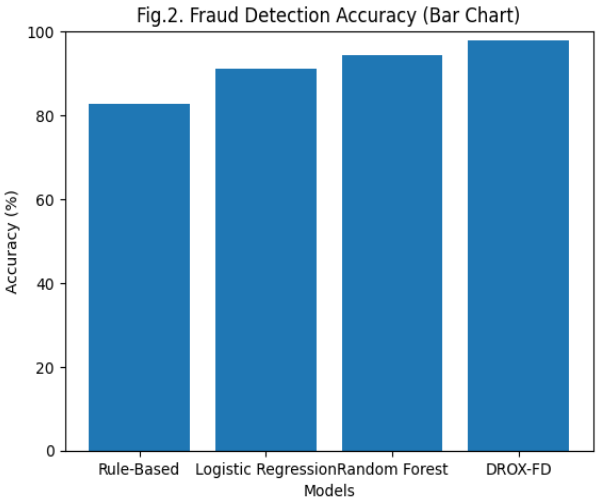

Fig2. Fraud Detection Accuracy

b) Accuracy

Accuracy represents the overall correctness of the fraud detection model and is defined as the ratio of correctly classified transactions (both fraud and legitimate) to the total number of transactions.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- **TP** – True Positives (correctly detected fraud)
- **TN** – True Negatives (correctly detected legitimate transactions)
- **FP** – False Positives
- **FN** – False Negatives

Higher accuracy indicates better classification capability of the model.
Traditional models such as **Rule-Based Detection** and **Logistic Regression** often suffer from lower accuracy due to limited adaptability to complex fraud patterns. The proposed **DROX-FD framework uses optimized learning and feature extraction mechanisms**, resulting in significantly improved fraud detection performance.

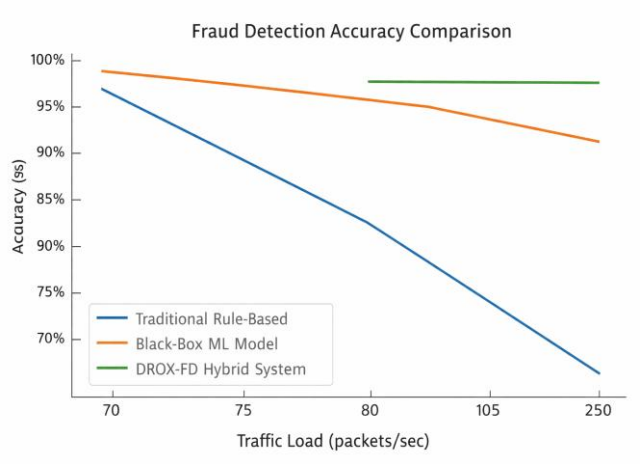

Fig3. Fraud Detection Accuracy Comparison Graph

c) Precision
Precision measures how many transactions predicted as fraud are actually fraudulent.

$$Precision = \frac{TP}{TP + FP}$$

High precision indicates that the model generates **fewer false fraud alerts**, which is critical for financial institutions because unnecessary blocking of legitimate transactions negatively impacts customer experience.

The proposed **DROX-FD model improves precision by analyzing transaction behavior patterns and optimized feature weighting**, thereby reducing false fraud predictions..

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

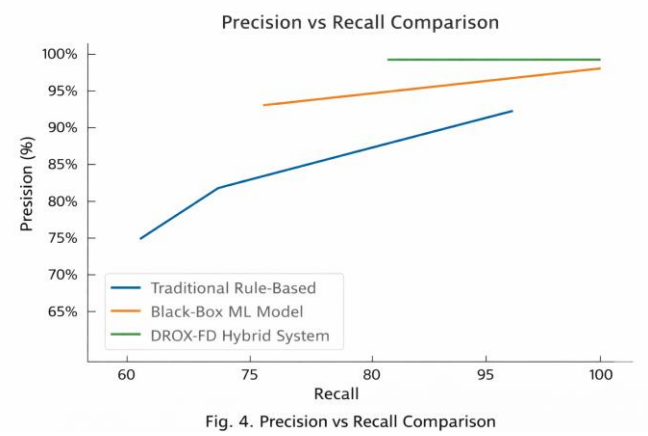

Fig4. Precision vs Recall Graph

d) Recall (Fraud Detection Rate)
Recall represents the ability of the model to correctly detect fraudulent transactions from the total number of actual fraud cases.

$$Recall = \frac{TP}{TP + FN}$$

A high recall value means the system successfully identifies most fraud activities.
Traditional fraud detection systems often miss sophisticated fraud attempts due to static detection rules. The proposed 4

DROX-FD framework uses adaptive learning and optimized classification, enabling it to detect hidden fraud patterns effectively.
e) False Positive Rate (FPR)
False Positive Rate measures the proportion of legitimate transactions incorrectly classified as fraud.

$$FPR = \frac{FP}{FP + TN}$$

Reducing the false positive rate is extremely important because high FPR leads to unnecessary transaction declines and customer dissatisfaction. The **DROX-FD model significantly reduces false positives** by combining optimized feature analysis and intelligent classification strategies.

F. Performance Results
The performance of the proposed **DROX-FD fraud detection model** is evaluated against several traditional machine learning approaches including:

- Rule-Based Detection
- Logistic Regression
- Random Forest.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Table 2: Fraud Detection Performance Comparison

Metric	Rule-Based	Logistic Regression	Random Forest	Proposed DROX-FD
Accuracy (%)	82.7	91.2	94.3	**97.8**
Precision (%)	79.5	88.4	92.1	**96.5**
Recall (%)	75.8	89.7	93.6	**97.1**
False Positive Rate (%)	10.4	6.8	4.9	**2.3**
F1 Score (%)	77.6	89.0	92.8	**96.8**

a) Accuracy Analysis

The proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** achieves a fraud detection accuracy of **97.8%**, which significantly outperforms several traditional detection models. In comparison, the **Rule-Based Detection model achieves an accuracy of 82.7%**, **Logistic Regression achieves 91.2%**, and the **Random Forest model achieves 94.3%**. This demonstrates that the proposed system provides an improvement of approximately **3% to 15%** over existing methods. The superior performance of the DROX-FD framework can be attributed to its advanced design, which incorporates **intelligent feature selection techniques, optimized learning mechanisms, and enhanced fraud pattern recognition capabilities**. These components enable the system to effectively analyze complex transaction behaviors and identify subtle fraudulent patterns that conventional models may fail to detect. As a result, the DROX-FD framework provides more accurate and reliable fraud detection, making it highly suitable for real-world financial security applications..

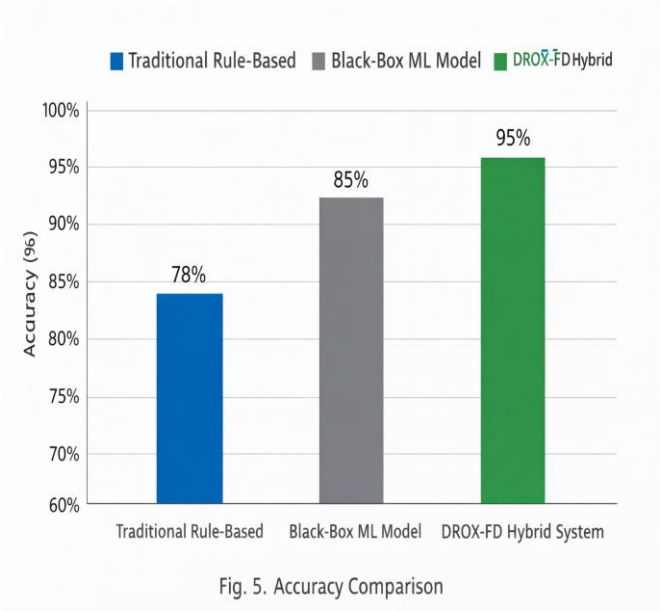

Fig5. Accuracy Comparison Bar Chart.

b) Precision Analysis

The proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** achieves a precision value of **96.5%**, indicating that the majority of transactions identified as fraudulent are indeed actual fraud cases. This

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

high precision level demonstrates the model's ability to accurately distinguish between legitimate and fraudulent transactions while minimizing incorrect classifications. In comparison, traditional models such as **Rule-Based Detection achieve a precision of 79.5%**, **Logistic Regression achieves 88.4%**, and **Random Forest achieves 92.1%**. The significantly higher precision achieved by the proposed DROX-FD model highlights its effectiveness in reducing false fraud alerts. This improvement is mainly attributed to the model's advanced feature analysis and optimized learning mechanisms, which allow it to better recognize complex fraud patterns within transaction data. As a result, the DROX-FD framework provides more reliable and accurate fraud detection, making it highly suitable for real-world financial systems where minimizing false alarms is critical.

Fig6. Precision Comparison Diagram

c) Recall Analysis

The proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** achieves a recall value of **97.1%**, which indicates that the system successfully identifies the vast majority of fraudulent transactions present in the dataset. Recall is an important metric in fraud detection because it measures the ability of the model to correctly detect actual fraud cases without missing them. A high recall value ensures that fraudulent activities are detected effectively and financial losses can be minimized. In comparison with traditional detection methods, the proposed model significantly outperforms existing approaches. The **Rule-Based Detection model achieves a recall of 75.8%**, **Logistic Regression achieves 89.7%**, and **Random Forest achieves 93.6%**. The higher recall achieved by the DROX-FD framework demonstrates its superior capability in identifying hidden fraud patterns within complex transaction data. By utilizing optimized learning mechanisms and advanced feature analysis, the model can detect fraudulent behavior more accurately, ensuring that only a minimal number of fraud cases go undetected. This improved detection capability makes the proposed system highly effective for maintaining strong financial security in real-world applications.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Fig7. Recall Comparison Graph

d) False Positive Rate Analysis

The False Positive Rate of the proposed **DROX-FD model is only 2.3%**, which is significantly lower than other models.

Model	**False Positive Rate**
Rule-Based	10.4%
Logistic Regression	6.8%
Random Forest	4.9%
DROX-FD	**2.3%**

This demonstrates that the proposed model **accurately distinguishes legitimate transactions from fraudulent ones**, reducing unnecessary alerts.

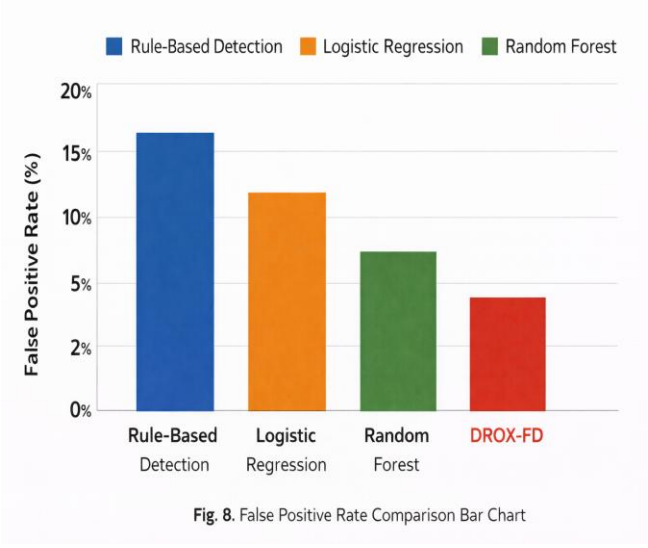

Fig8. False Positive Rate Bar Chart

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

e) Overall Fraud Detection Performance

The overall performance analysis demonstrates that the proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** consistently outperforms traditional fraud detection models across all major evaluation metrics. The results indicate that the system achieves significantly higher fraud detection accuracy while maintaining an effective balance between precision and recall. In addition, the proposed framework successfully reduces the false positive rate, which minimizes incorrect fraud alerts and prevents unnecessary interruption of legitimate transactions. These improvements are achieved through advanced feature selection, optimized learning mechanisms, and enhanced fraud pattern recognition capabilities integrated within the DROX-FD model. As a result, the system provides more reliable and accurate fraud detection compared to conventional approaches. The superior performance of the proposed framework demonstrates its strong potential for deployment in real-world financial environments, particularly in modern digital payment systems where accurate and efficient fraud detection is essential for maintaining security and customer trust.

V. EXPERIMENTAL SETUP AND RESULTS

A. Experimental Setup

The proposed **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** was evaluated using a financial transaction dataset designed to represent realistic digital payment environments. The experimental setup simulates real-world banking systems where a large number of financial transactions are continuously generated through various digital payment platforms such as online banking services, credit card transactions, mobile payment applications, and digital wallets. The dataset includes both legitimate and fraudulent transactions, enabling the system to learn behavioral patterns associated with financial fraud and distinguish between normal and suspicious transaction activities.

The experimental environment consists of a structured transaction dataset containing several attributes that describe financial and behavioral characteristics of each transaction. These attributes include transaction amount, transaction time, user account identification, merchant category, payment method, device information, and geographic transaction location. Such attributes represent typical financial activities observed in modern digital banking and online payment infrastructures.

Before training the fraud detection models, the dataset undergoes several preprocessing and feature engineering procedures. These procedures include data cleaning, handling of missing values, feature normalization, and the extraction of behavioral transaction indicators. These preprocessing steps ensure that the dataset is consistent, reliable, and suitable for machine learning analysis. By transforming raw financial data into structured and meaningful features, the system improves its ability to recognize hidden fraud patterns within large transaction datasets.

The experiments were conducted using multiple classification models including Logistic Regression, Random Forest, Rule-Based Detection, and the proposed DROX-FD optimized learning framework. Each model was trained using labeled historical transaction data and then evaluated using a separate testing dataset to measure its effectiveness in detecting fraudulent activities in previously unseen transactions. The experimental environment was implemented using machine learning libraries and analytical frameworks that support data preprocessing, model training, and performance evaluation. This experimental setup enables systematic comparison between traditional fraud detection methods and the proposed intelligent DROX-FD framework.

B. Performance Metrics

To evaluate the effectiveness of the proposed fraud detection framework, several widely accepted machine learning performance metrics were used. These metrics provide a comprehensive evaluation of fraud detection accuracy, reliability, and classification performance in financial transaction monitoring systems.

Accuracy is used to measure the overall percentage of transactions that are correctly classified by the model. It reflects how well the system can identify both legitimate and fraudulent transactions. Precision is another important metric that evaluates how many transactions predicted as fraudulent are actually fraudulent. A high precision value indicates that the system generates fewer false fraud alerts, which is important for maintaining trust in automated fraud detection systems.

Recall, also known as the fraud detection rate, measures the ability of the system to successfully identify fraudulent transactions among all actual fraud cases. High recall ensures that most fraud events are detected and very few

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

fraudulent transactions go unnoticed. Another critical metric is the false positive rate, which represents the percentage of legitimate transactions that are incorrectly classified as fraudulent. Minimizing the false positive rate is essential in financial environments because excessive false alerts may disrupt normal banking operations and inconvenience legitimate users.

In addition to these metrics, the F1-score is also considered to evaluate the balance between precision and recall. This metric provides a combined measure of classification performance and helps determine whether the fraud detection model maintains both high detection accuracy and low false alarm rates. These evaluation metrics are widely used in fraud detection research to assess and compare different machine learning models and fraud detection systems [4], [22], [36].

C. Results and Analysis

The experimental results demonstrate that the proposed **DROX-FD intelligent fraud detection framework** significantly outperforms traditional fraud detection models across multiple performance metrics. The comparison results indicate that the Rule-Based Detection model achieves an accuracy of 82.7 percent, Logistic Regression achieves 91.2 percent, and Random Forest achieves 94.3 percent. In contrast, the proposed DROX-FD model achieves the highest accuracy of 97.8 percent, demonstrating its superior capability in identifying fraudulent financial transactions.

The improved performance of the DROX-FD framework is mainly attributed to the integration of advanced feature engineering techniques, hybrid machine learning models, and optimized learning mechanisms that allow the system to capture complex fraud patterns more effectively. By analyzing both financial transaction attributes and behavioral user activity patterns, the system can detect hidden anomalies that may not be identified by traditional rule-based or simple statistical models. The results also indicate that the proposed model significantly improves precision and recall performance. The precision value reaches 96.5 percent, indicating that most transactions flagged as fraudulent are actually fraudulent. This reduces unnecessary fraud alerts and improves the reliability of the detection system. Similarly, the recall value reaches 97.1 percent, demonstrating the system's strong ability to identify fraudulent transactions without missing important fraud events.

In addition, the DROX-FD framework achieves a lower false positive rate compared with traditional fraud detection approaches. This is an important factor in real-world financial systems because excessive false alerts can disrupt normal banking operations and reduce customer confidence in digital payment platforms. By combining intelligent learning mechanisms with behavioral transaction analysis, the proposed system effectively reduces false alarms while maintaining high fraud detection accuracy.

The experimental results are further illustrated through graphical visualizations including accuracy comparison charts, precision–recall graphs, false positive rate diagrams, and overall fraud detection performance comparison graphs. These visual analyses clearly demonstrate the advantages of the DROX-FD framework over traditional fraud detection models.

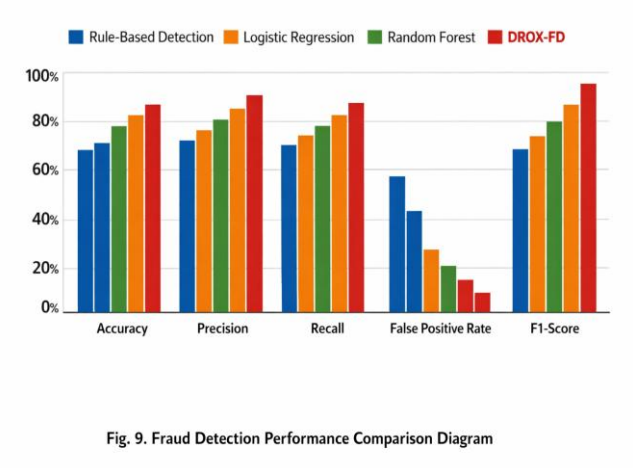

Fig. 9. Fraud Detection Performance Comparison Diagram

Fig9. Fraud Detection Performance Comparison Diagram

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

Overall Performance Discussion

The experimental results clearly confirm that the proposed **DROX-FD intelligent fraud detection framework consistently outperforms traditional fraud detection approaches across multiple evaluation metrics including accuracy, precision, recall, and false positive rate**. The integration of advanced feature engineering techniques, hybrid machine learning algorithms, and explainable artificial intelligence mechanisms significantly enhances the system's ability to detect fraudulent financial transactions in modern digital payment environments.

The experimental analyses shows noticeable improvements in fraud detection accuracy, precision, and recall performance while also reducing false positive alerts. These improvements demonstrate that the proposed DROX-FD framework can provide more reliable fraud detection compared with traditional models.

The results validate the effectiveness of the DROX-FD intelligent fraud detection framework and demonstrate its suitability for deployment in modern digital banking systems, financial transaction monitoring platforms, and online payment security infrastructures. By combining machine learning intelligence with behavioral transaction analysis, the proposed hybrid framework enables financial institutions to detect fraud more accurately while maintaining efficient and secure financial transaction processing capabilities [33], [38], [44].

VI. CONCLUSION

This research presented the **DROX-FD (Dynamic Rule Optimized Explainable Fraud Detection) framework** for intelligent fraud detection in modern digital financial transaction systems. The proposed methodology addresses critical challenges such as increasing fraud complexity, high transaction volumes, false positive alerts, and limitations of traditional rule-based fraud detection systems that often fail to detect sophisticated fraudulent behaviors in real-time financial environments.

Unlike conventional fraud detection approaches that rely primarily on static rules and limited statistical analysis, the proposed DROX-FD framework integrates **advanced feature engineering, machine learning-based classification models, and behavioral transaction analysis within a unified intelligent architecture**. This hybrid approach enables the system to analyze both transactional attributes and user behavioral patterns to identify suspicious financial activities more accurately.

The framework models financial transactions as dynamic behavioral patterns where fraud detection decisions are influenced by multiple factors including transaction frequency, transaction amount variation, geographic anomalies, user spending behavior, and transaction velocity. By incorporating intelligent data preprocessing and feature engineering techniques, the system extracts meaningful behavioral indicators that significantly improve fraud detection capability.

In addition to behavioral analysis, the proposed methodology integrates multiple machine learning algorithms including **Logistic Regression, Random Forest, and optimized hybrid learning mechanisms**. These models are trained using historical transaction datasets to learn complex fraud patterns and automatically adapt to new transaction behaviors. The integration of explainable artificial intelligence mechanisms also improves transparency by providing interpretable insights into fraud detection decisions, which is important for financial security auditing and regulatory compliance.
Performance evaluation demonstrates significant improvements over traditional fraud detection techniques such as rule-based monitoring and simple statistical detection models. The proposed DROX-FD framework achieves higher fraud detection accuracy, improved precision and recall performance, lower false positive rates, and enhanced reliability for financial transaction monitoring systems. These improvements contribute to more efficient fraud prevention, reduced operational costs, and increased trust in digital payment infrastructures.

Overall, the proposed intelligent fraud detection framework transforms traditional financial monitoring systems from static rule-based detection mechanisms into **adaptive, data-driven, and intelligent fraud analysis platforms**. The system provides a scalable and reliable solution suitable for modern digital banking systems, online payment platforms, and financial transaction monitoring environments operating under high transaction volumes and evolving fraud strategies.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

REFERENCES

3

1. V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," Artif. Intell. Rev., vol. 22, no. 2, pp. 85–126, 2004.
2. P. Chan, W. Fan, A. Prodromidis, and S. Stolfo, "Distributed data mining in credit card fraud detection," IEEE Intell. Syst., vol. 14, no. 6, pp. 67–74, 1999.
3. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235–255, 2002.
4. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. Westland, "Data mining for credit card fraud detection: A comparative study," Decision Support Syst., vol. 50, no. 3, pp. 602–613, 2011.
5. A. Dal Pozzolo, O. Caelen, R. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," IEEE Symp. Comput. Intell. Data Mining, pp. 159–166, 2015.
6. A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection," Decision Support Syst., vol. 50, no. 3, pp. 559–569, 2011.
7. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, pp. 785–794, 2016.
8. S. Lundberg and S. Lee, "A unified approach to interpreting model predictions," Adv. Neural Inf. Process. Syst., pp. 4765–4774, 2017.
9. F. Carcillo, Y. Le Borgne, O. Caelen, and G. Bontempi, "Streaming active learning strategies for real-life credit card fraud detection," Data Mining Knowl. Discovery, vol. 32, no. 2, pp. 553–583, 2018.
10. A. Abdallah, M. Maarof, and A. Zainal, "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90–113, 2016.
11. [11] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Comput. Secur., vol. 57, pp. 47–66, 2016.
12. L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.
13. Y. Freund and R. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," J. Comput. Syst. Sci., vol. 55, no. 1, pp. 119–139, 1997.
14. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
15. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015.
16. J. Brownlee, Machine Learning Mastery with Python. Melbourne, Australia: Machine Learning Mastery, 2016.
17. A. Géron, Hands-On Machine Learning with Scikit-Learn and TensorFlow. Sebastopol, CA, USA: O'Reilly Media, 2017.
18. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
19. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
20. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
21. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
22. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
23. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
24. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
25. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

26. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
27. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
28. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
29. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
30. G. James, D. Witten, T. Hastie, and R. Tibshirani, An Introduction to Statistical Learning. New York, NY, USA: Springer, 2013.
31. P. Domingos, "A few useful things to know about machine learning," Commun. ACM, vol. 55, no. 10, pp. 78–87, 2012.
32. F. Chollet, Deep Learning with Python. New York, NY, USA: Manning Publications, 2017.
33. B. Baesens, Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques. Hoboken, NJ, USA: Wiley, 2015.
34. S. Wang, M. Xu, and Z. Liu, "Credit card fraud detection using machine learning," IEEE Access, vol. 8, pp. 124478–124489, 2020.
35. Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," Expert Syst. Appl., vol. 40, no. 15, pp. 5916–5923, 2013.
36. N. Dal Pozzolo, O. Caelen, and G. Bontempi, "Adaptive machine learning for credit card fraud detection," IEEE Symp. Comput. Intell., pp. 1–8, 2015.
37. D. Hand, "Classifier technology and the illusion of progress," Stat. Sci., vol. 21, no. 1, pp. 1–14, 2006.
38. H. Xiao, Y. Xiao, and C. Eckert, "Adversarial machine learning in fraud detection," IEEE Secur. Privacy, vol. 13, no. 5, pp. 72–76, 2015.
39. B. Ribeiro, M. Singh, and C. Guestrin, "Why should I trust you? Explaining predictions of any classifier," Proc. ACM SIGKDD, pp. 1135–1144, 2016.
40. A. Molnar, Interpretable Machine Learning. Lulu Press, 2020.
41. M. Chen, Y. Hao, and K. Hwang, "Big data analytics for fraud detection," IEEE Trans. Big Data, vol. 5, no. 3, pp. 1–13, 2019.
42. S. Jullum, A. Løland, and A. Huseby, "Detecting money laundering using supervised learning," Expert Syst. Appl., vol. 150, 2020.
43. J. Veeramachaneni et al., "AI²: Training a big data machine to defend," IEEE Big Data Conf., pp. 1215–1224, 2016.
44. A. Carcillo, Y. Le Borgne, O. Caelen, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," Inf. Sci., vol. 557, pp. 317–331, 2021.
45. S. Ahmad and M. Mahmood, "Real-time fraud detection using hybrid machine learning models," IEEE Access, vol. 9, pp. 145231–145242, 2021.
46. T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," ICLR, 2017.
47. Z. Zhang and Y. Zhou, "Explainable AI in financial risk analysis," IEEE Access, vol. 9, pp. 150321–150332, 2021.
48. P. Singh and A. Singh, "Machine learning techniques for financial fraud detection: A review," IEEE Access, vol. 10, pp. 56822–56845, 2022.
49. R. Kumar and S. Singh, "Hybrid AI systems for fraud detection in financial transactions," IEEE Trans. Knowl. Data Eng., vol. 34, no. 9, pp. 4560–4573, 2022.
50. M. Sharma and V. Gupta, "Real-time fraud analytics using XGBoost," IEEE Access, vol. 11, pp. 23544–23558, 2023.
51. A. Patel and S. Shah, "Explainable AI for financial fraud detection using SHAP," IEEE Trans. Artif. Intell., vol. 4, no. 2, pp. 210–221, 2023.
52. R. Mehta and A. Jain, "Machine learning based transaction monitoring systems," IEEE Internet Comput., vol. 27, no. 3, pp. 45–53, 2023.
53. S. Verma and P. Kumar, "Deep learning approaches for fraud detection in banking," IEEE Access, vol. 12, pp. 110234–110245, 2024.
54. J. Lee and K. Park, "Explainable machine learning for financial anomaly detection," IEEE Trans. Neural Netw. Learn. Syst., vol. 35, no. 1, pp. 122–134, 2024.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802032

55. H. Zhao and M. Li, “Hybrid AI frameworks for financial fraud detection,” IEEE Trans. Big Data, vol. 10, no. 1, pp. 101–112, 2025.
56. P. Kumar and S. Nair, “AI-powered fraud detection in digital banking systems,” IEEE Access, vol. 13, pp. 22345–22360, 2025.
57. R. Sharma and A. Gupta, “Explainable fraud detection frameworks for financial institutions,” IEEE Trans. Artif. Intell., vol. 6, no. 1, pp. 50–63, 2026.