© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720044

A Machine Learning Framework for Financial Fraud Detection Using Credit Card Transaction Data

YAHUZA NAFIU[1], PROF. AHMAD BAITA GARKO[2], DR. ABUBAKAR ATIKU MUSLIM[3]
[1]*Department of Computer Science, Federal University Birnin Kebbi, Kebbi State, Nigeria*
[2]*Department of Computer Science, Federal University Dutsin-Ma (FUDMA) Dutsinma, Katsina State, Nigeria.*
[3]*Abdullahi Fodio University of science and Technology Aliero, Kebbi State Nigeria*

Abstract- ***Financial fraud has become one of the most significant challenges confronting modern electronic payment systems, resulting in substantial financial losses for individuals and financial institutions worldwide. The increasing volume of digital financial transactions necessitates intelligent fraud detection systems capable of accurately distinguishing fraudulent transactions from legitimate ones. This study proposes a machine learning framework for financial fraud detection using a publicly available credit card transaction dataset obtained from Kaggle. The research focuses on analyzing the characteristics of financial transaction data and developing a robust framework for fraud detection through systematic data preprocessing and feature engineering. The methodology involved duplicate removal, feature scaling using StandardScaler, creation of a transaction-hour feature and class balancing using the Synthetic Minority Over-sampling Technique (SMOTE) to address the severe class imbalance inherent in fraud datasets. The processed data were integrated into a structured machine learning framework designed to support fraud detection and future model deployment. The proposed framework provides a comprehensive workflow encompassing data acquisition, preprocessing, feature engineering, model development and evaluation. The developed architecture enhances data quality, improves model readiness, and establishes a reliable foundation for implementing intelligent fraud detection systems in financial environments. The study contributes a scalable and practical machine learning framework that can be adapted for real-world financial transaction monitoring and future intelligent fraud prevention applications.***

Keywords: Financial Fraud Detection, Machine Learning, Credit Card Transactions, Data Preprocessing, SMOTE

I. INTRODUCTION

The rapid growth of electronic payment systems, online banking, mobile commerce, and digital financial services has significantly transformed the global financial sector. Although these technological advancements have improved the speed, convenience, and accessibility of financial transactions, they have also increased the vulnerability of financial systems to fraudulent activities. Financial fraud, particularly credit card fraud, has become one of the most persistent challenges facing financial institutions, businesses, and consumers worldwide. Fraudulent transactions result in substantial economic losses, undermine customer confidence, and threaten the integrity of digital payment infrastructures.

The increasing volume and complexity of financial transactions have made traditional fraud detection techniques, such as manual auditing and rule-based systems, less effective. Conventional approaches often struggle to detect evolving fraud patterns because fraudsters continuously modify their strategies to evade predefined rules. As a result, there has been growing interest in applying Artificial Intelligence (AI) and Machine Learning (ML) techniques to automate fraud detection by learning complex transaction patterns and identifying suspicious activities with minimal human intervention. Recent studies have demonstrated that machine learning algorithms can effectively distinguish fraudulent transactions from legitimate ones by analyzing historical transaction data and recognizing hidden behavioural patterns (Dal Pozzolo et al., 2018; Hernandez Aros et al., 2024; Almalki & Masud, 2025).

One of the major challenges in financial fraud detection is the highly imbalanced nature of transaction datasets, where legitimate transactions significantly outnumber fraudulent ones. Such imbalance often biases machine learning models toward the majority class, resulting in poor fraud

detection performance despite achieving high overall accuracy. Consequently, effective preprocessing techniques, including feature scaling, feature engineering, duplicate removal, and class balancing methods such as the Synthetic Minority Over-sampling Technique (SMOTE), have become essential for improving model learning and enhancing fraud detection capability (Chawla et al., 2002; Thivaios et al., 2026).

In addition to data preprocessing, the development of a structured machine learning framework plays a critical role in ensuring the successful implementation of fraud detection systems. A well-designed framework integrates data acquisition, preprocessing, feature engineering, model development, and evaluation into a unified workflow that facilitates efficient fraud analysis and supports future deployment in real-world financial environments. Such frameworks improve reproducibility, scalability, and the practical applicability of machine learning-based fraud detection solutions.

This study proposes a comprehensive machine learning framework for financial fraud detection using a publicly available credit card transaction dataset. The proposed framework incorporates data cleaning, duplicate removal, feature scaling, engineered temporal features, and SMOTE-based class balancing to prepare transaction data for intelligent fraud detection. Unlike studies that primarily focus on comparing classifier performance, this research emphasizes the development of a robust preprocessing pipeline and a modular framework capable of supporting reliable fraud detection applications. The framework provides a systematic foundation for subsequent model development and deployment in financial transaction monitoring systems.

The remainder of this paper is organized as follows. Section 2 reviews related studies on financial fraud detection and machine learning applications. Section 3 presents the materials and methods, including dataset description, preprocessing techniques, feature engineering, and the proposed machine learning framework. Section 4 discusses the proposed framework and its practical implications, while Section 5 concludes the paper and outlines future research directions.

II. RELATED WORK

Financial fraud detection has attracted considerable attention from researchers due to the rapid growth of electronic payment systems and the increasing sophistication of fraudulent activities. Machine learning techniques have emerged as effective solutions because of their ability to automatically learn transaction patterns and distinguish fraudulent activities from legitimate financial transactions.

Ngai et al. (2011) conducted one of the earliest comprehensive reviews of data mining techniques for financial fraud detection. Their study demonstrated that machine learning algorithms, including Decision Trees, Logistic Regression, and Artificial Neural Networks, significantly improved fraud detection performance compared with traditional statistical methods. However, the review highlighted the need for more scalable and adaptive fraud detection systems capable of handling large financial datasets.

Abdallah et al. (2016) conducted a comprehensive survey of financial fraud detection systems, reviewing both traditional statistical methods and intelligent computational techniques used in fraud detection applications. The authors highlighted the growing complexity of financial fraud and emphasized that machine learning approaches have become increasingly effective due to their ability to learn hidden patterns from large transaction datasets. The study also identified several challenges, including class imbalance, evolving fraud patterns, and the need for adaptive detection models capable of responding to emerging fraud strategies. However, the survey was primarily theoretical and did not experimentally evaluate or compare machine learning algorithms using real financial transaction datasets. The present study builds upon these observations by developing and evaluating a practical machine learning framework using real-world credit card transaction data while incorporating preprocessing techniques, class balancing using SMOTE, and comprehensive performance evaluation.

West and Bhattacharya (2016) presented a comprehensive review of intelligent financial fraud detection techniques, focusing on the application of machine learning and data mining methods in financial

security. The review demonstrated that intelligent learning algorithms outperform traditional rule-based systems in identifying fraudulent financial transactions due to their capability to model complex relationships within large datasets. Nevertheless, the authors identified several limitations affecting practical implementation, including limited model interpretability, class imbalance, and difficulties associated with deploying fraud detection systems in operational financial environments. These observations support the motivation for the present study, which proposes a structured machine learning framework that integrates preprocessing, feature engineering, class balancing, and system architecture to improve the practical applicability of financial fraud detection systems.

Dal Pozzolo et al. (2018) investigated the challenges associated with highly imbalanced credit card transaction datasets. Their research demonstrated that addressing class imbalance is essential for improving fraud detection performance and reducing false negative predictions. The study emphasized the importance of appropriate sampling techniques and robust evaluation metrics when developing fraud detection models.

Carcillo et al. (2019) proposed a hybrid fraud detection approach that combines supervised and unsupervised machine learning techniques to improve credit card fraud detection performance. The study demonstrated that integrating anomaly detection with supervised classification enables the identification of both previously known and emerging fraud patterns. The authors further highlighted the importance of handling highly imbalanced transaction datasets and adapting fraud detection models to continuously evolving fraud behaviors. Despite its strong predictive capability, the proposed approach involved relatively complex model integration, which may increase computational requirements and implementation complexity in operational financial systems. The present study adopts a simpler yet effective supervised learning framework enhanced through preprocessing, feature engineering, SMOTE-based balancing, and systematic model evaluation to achieve reliable fraud detection performance while maintaining implementation simplicity.

Arrieta et al. (2020) presented a comprehensive review of Explainable Artificial Intelligence (XAI), discussing various techniques developed to improve the transparency, interpretability, and accountability of artificial intelligence systems. The authors argued that as machine learning models become increasingly complex, understanding how prediction decisions are generated is essential for building trust in high-risk application domains such as finance, healthcare, and cybersecurity. Although the study established a strong theoretical foundation for explainable AI, it was not specifically designed for financial fraud detection and did not propose an operational fraud detection framework. The present study focuses primarily on developing a structured machine learning framework for financial fraud detection while recognizing explainability as an important direction for future research and system enhancement.

Sadineni (2020) developed a credit card fraud detection system using multiple supervised machine learning algorithms, including Artificial Neural Networks (ANN), Decision Trees (DT), Support Vector Machines (SVM), Logistic Regression (LR), and Random Forest (RF). The study employed Principal Component Analysis (PCA) for feature extraction and evaluated model performance using Accuracy, Precision, and False Alarm Rate. Experimental results indicated that the Artificial Neural Network achieved the highest prediction accuracy among the evaluated models. Although the study provided a useful comparative evaluation of machine learning algorithms, it did not address class imbalance using oversampling techniques, incorporate cross-validation, or simulate real-time fraud detection. Shakeabubakor (2024) proposed an integrated framework for real-time financial fraud detection by combining machine learning techniques with cloud-based data warehousing technologies. The study demonstrated that cloud computing environments facilitate rapid processing of financial transactions while supporting scalable fraud detection systems capable of handling large transaction volumes. The research emphasized the importance of real-time monitoring in minimizing financial losses caused by fraudulent activities. However, the study provided limited discussion on feature engineering, class imbalance handling, and comparative evaluation of multiple machine learning algorithms. Building upon

this work, the present study introduces comprehensive preprocessing techniques, SMOTE-based class balancing, and a structured machine learning framework designed to improve fraud detection reliability while supporting future real-time deployment.

Rao and Mandhala (2024) conducted a comprehensive review of machine learning and data mining techniques applied to financial fraud detection. The study examined various supervised and unsupervised learning algorithms, highlighting their strengths, limitations, and suitability for different fraud detection scenarios. The authors concluded that although machine learning has significantly improved fraud detection accuracy, challenges remain regarding scalability, model interpretability, class imbalance, and deployment in dynamic financial environments. Since the study was primarily a review, it did not develop or experimentally validate a fraud detection framework. The present study addresses these research gaps by proposing and implementing a structured machine learning framework that integrates preprocessing, feature engineering, class balancing, and performance evaluation using real financial transaction data.

Preciado Martínez et al. (2025) performed a comparative analysis of several machine learning algorithms for detecting fraudulent banking transactions. The study evaluated the predictive performance of different classification models using standard performance metrics and reported that ensemble learning methods generally achieved superior fraud detection accuracy compared with conventional classification algorithms. The authors also emphasized the importance of selecting appropriate machine learning models based on dataset characteristics and operational requirements. Nevertheless, the research focused primarily on comparative model evaluation and did not propose a comprehensive fraud detection framework that integrates preprocessing, feature engineering, and deployment considerations. The present study extends this line of research by developing a modular machine learning framework that incorporates comprehensive preprocessing, SMOTE-based balancing, feature engineering, and system architecture to improve the effectiveness and practical applicability of fraud detection systems.

Recent studies have focused on improving the transparency, robustness, and practical applicability of machine learning-based fraud detection systems. Hernandez Aros et al. (2024) reported that machine learning techniques significantly enhance financial fraud detection capabilities but emphasized the need for improved real-world deployment strategies and scalable fraud detection frameworks. Similarly, Chiaburu et al. (2024) highlighted the importance of explainable artificial intelligence (XAI) in increasing user confidence and supporting decision-making in intelligent financial systems.

Unlike Almalki and Masud (2025), who focused on integrating explainable artificial intelligence with stacking ensemble methods to improve prediction transparency, the present study emphasizes the development of a comprehensive fraud detection framework that combines data preprocessing, feature engineering, SMOTE-based class balancing, modular system architecture, and comparative evaluation of multiple machine learning algorithms. This broader methodological approach improves the framework's applicability for practical fraud detection system development while providing a foundation for future integration of explainable AI techniques.

Thivaios et al. (2026) presented a comprehensive survey of machine learning and deep learning techniques for financial fraud detection. The study reviewed various fraud detection architectures, data modalities, and deployment challenges associated with intelligent financial systems. The authors concluded that while machine learning models have significantly improved fraud detection accuracy, future research should focus on scalable system architectures, explainable artificial intelligence, graph-based learning, and real-time deployment frameworks. These recommendations support the motivation for the present study, which proposes a structured machine learning framework capable of supporting practical financial fraud detection applications.

Motivated by these studies, the present research proposes a comprehensive machine learning

framework that integrates duplicate removal, feature scaling, temporal feature engineering, and SMOTE-based class balancing before model development. Unlike previous studies that primarily emphasized algorithm comparison, the proposed framework focuses on establishing a structured preprocessing and development pipeline that improves data quality, enhances model readiness, and supports future deployment within practical financial fraud detection environments.

Table 1. Summary of Related Studies

Author(s)	Year	Focus	Limitation
Ngai et al.	2011	Data mining for financial fraud detection	Limited discussion of modern ML techniques
Dal Pozzolo et al.	2018	Class imbalance in credit card fraud	Focused mainly on sampling techniques
Sadineni	2020	ML comparison for fraud detection	No SMOTE, no cross-validation, no real-time simulation
Hernandez Aros et al.	2024	Machine learning in financial fraud	Recommended practical deployment improvements
Chiaburu et al.	2024	Explainable AI	Limited focus on fraud detection implementation
Almalki & Masud	2025	Explainable AI framework for financial fraud detection	Did not emphasize preprocessing, SMOTE, cross-validation, or real-time simulation
Thivaios et al.	2026	Survey of ML and DL techniques, architectures, and deployment challenges	Review paper only; no implementation or experimental validation

2.2 Research Gaps

The reviewed literature demonstrates that machine learning has become one of the most effective approaches for financial fraud detection due to its ability to identify complex transaction patterns and improve fraud classification accuracy. Early studies by Abdallah et al. (2016) and West and Bhattacharya (2016) established the importance of intelligent fraud detection systems and highlighted the growing need for adaptive machine learning techniques capable of addressing increasingly sophisticated financial fraud. However, these studies were primarily review-based and did not develop or experimentally validate practical fraud detection frameworks.

Subsequent studies focused on improving specific components of fraud detection systems. Bahnsen et al. (2016) demonstrated the importance of feature engineering in enhancing predictive performance, while Carcillo et al. (2019) proposed a hybrid learning approach that combined supervised and unsupervised learning techniques for fraud detection. Although these studies improved model performance, they provided limited emphasis on developing comprehensive machine learning frameworks that integrate preprocessing, feature engineering, class balancing, and deployment considerations into a unified architecture.

Recent studies have further expanded financial fraud detection research by incorporating explainable artificial intelligence, cloud computing, and advanced machine learning techniques. Arrieta et al. (2020) emphasized the importance of Explainable Artificial Intelligence (XAI) for improving model transparency, whereas Shakeabubakor (2024) proposed a cloud-based framework for real-time financial fraud detection. Similarly, Rao and Mandhala (2024) reviewed modern machine learning and data mining techniques, identifying challenges related to scalability, class imbalance, and deployment in dynamic financial environments. More recently, Preciado Martínez et al. (2025) compared the predictive performance of several machine learning algorithms for banking fraud detection but concentrated primarily on algorithm evaluation rather

than the development of an integrated fraud detection framework.

Despite these contributions, several research gaps remain. First, many existing studies focus primarily on algorithm comparison without proposing a comprehensive framework that integrates data acquisition, preprocessing, feature engineering, class balancing, model development, prediction, and performance evaluation within a single workflow. Second, limited attention has been given to combining preprocessing techniques such as duplicate removal, feature scaling, engineered temporal features, and SMOTE-based class balancing to improve model readiness before classification. Third, while recent literature highlights the need for scalable and practical fraud detection systems, relatively few studies provide a structured system architecture that can support future deployment in operational financial environments. Finally, although recent research has increasingly emphasized explainability and real-time fraud detection, there remains a need for practical machine learning frameworks capable of supporting reliable fraud detection using real-world transaction datasets.

To address these gaps, the present study proposes a structured machine learning framework for financial fraud detection that integrates comprehensive preprocessing, feature engineering, SMOTE-based class balancing, modular system architecture, and performance evaluation using multiple machine learning models. By combining these components into a unified framework, the study aims to improve the robustness, scalability, and practical applicability of intelligent financial fraud detection systems.

III. MATERIALS AND METHODS

3.1 Research Design

This study adopted an experimental research design to develop a machine learning framework for financial fraud detection using historical credit card transaction data. The framework was designed to provide a systematic workflow for preparing financial transaction data before model development. The research focused on improving data quality through preprocessing and feature engineering while establishing a structured architecture capable of supporting intelligent fraud detection in financial systems. The methodology comprised data acquisition, preprocessing, feature engineering, class balancing, framework development, and system architecture design.

3.2 Dataset Description

The study utilized the publicly available Credit Card Fraud Detection dataset obtained from the Kaggle repository. The dataset contains 284,807 credit card transactions collected from European cardholders over two consecutive days. Each transaction is described using 31 attributes, including Time, Amount, Class, and twenty-eight anonymized numerical features (V1–V28) generated through Principal Component Analysis (PCA) to preserve customer confidentiality. The Class attribute represents the target variable, where legitimate transactions are labeled as 0 and fraudulent transactions as 1.

Following duplicate removal, the dataset contained 283,726 unique transactions, comprising 283,253 legitimate and 473 fraudulent transactions, highlighting the severe class imbalance typical of financial fraud datasets.

3.3 Data Preprocessing

Data preprocessing was performed to improve data quality and ensure suitability for machine learning. The following preprocessing operations were applied:

1. Loading the dataset into the Python environment.
2. Inspecting data types and descriptive statistics.
3. Detecting and removing duplicate records.
4. Confirming the absence of missing values.
5. Standardizing numerical features using the StandardScaler algorithm.
6. Separating predictor variables from the target class.
7. Partitioning the dataset into training and testing subsets using stratified sampling.

These preprocessing steps enhanced the consistency of the dataset and prepared it for subsequent feature engineering and machine learning model development.

3.4 Feature Engineering

Feature engineering was performed to improve the representational quality of the dataset. A new temporal feature (Hour) was extracted from the original Time

variable to capture transaction periods that may influence fraudulent behaviour. The engineered feature provides additional contextual information that may assist machine learning algorithms in distinguishing legitimate and fraudulent transactions.

To address the severe imbalance between legitimate and fraudulent transactions within the training data, the Synthetic Minority Over-sampling Technique (SMOTE) was employed. SMOTE generates synthetic minority-class observations, producing a balanced training dataset and reducing model bias toward the majority class. Previous studies have shown that class balancing significantly improves fraud detection performance in highly imbalanced datasets.

3.5 Proposed Machine Learning Framework

The proposed framework consists of five sequential stages:

1. Data Acquisition
2. Data Preprocessing
3. Feature Engineering and Class Balancing
4. Machine Learning Model Development
5. Fraud Prediction and System Evaluation

The framework provides a structured methodology for transforming raw financial transaction data into machine learning-ready datasets while ensuring scalability and reproducibility. It establishes a modular pipeline that can be extended for deployment in practical financial fraud detection environments.

Table 2: Summary of the proposed machine learning methodology for financial fraud detection.

Stage	Process	Technique/Tool Used	Output
1	Data Acquisition	Kaggle Credit Card Fraud Dataset	Raw transaction dataset
2	Data Cleaning	Duplicate removal, missing value inspection	Clean dataset
3	Feature Engineering	Hour feature extraction	Enhanced feature set
4	Feature Scaling	StandardScaler	Standardized numerical features
5	Data Splitting	Stratified Train-Test Split (70:30)	Training and testing datasets
6	Class Balancing	SMOTE	Balanced training dataset
7	Model Development	Machine learning model training	Trained fraud detection framework
8	Fraud Prediction	Binary Classification	Legitimate or Fraudulent transaction
9	Performance Evaluation	Accuracy, Precision, Recall, F1-Score, ROC-AUC	Model performance assessment

The methodology presented in Table 2 summarizes the sequential stages adopted in this study, beginning with data acquisition and ending with fraud prediction and model evaluation. Each stage contributes to improving data quality and establishing a reliable framework for machine learning-based financial fraud detection.

Table 3. Comparison of Existing Frameworks and the Proposed Framework

Study	Focus	Limitation	Improvement in This Study
Ngai et al. (2011)	Data mining framework	No real-time deployment	Proposed modular framework
Sadineni (2020)	ML comparison	No SMOTE, no framework	Added preprocessing, SMOTE, architecture
Hernandez Aros et al. (2024)	Literature review	No implementation	Developed practical framework
Thivaios et al. (2026)	Survey	No implementation	Developed and validated framework

3.6 Proposed Machine Learning Framework

The proposed machine learning framework was developed to provide a systematic and scalable approach for financial fraud detection using credit card transaction data. The framework integrates data acquisition, preprocessing, feature engineering, class balancing, model development, and fraud prediction into a unified workflow. By organizing these processes into sequential stages, the framework enhances data quality, improves model readiness, and supports reliable fraud detection in practical financial environments.

The framework begins with data acquisition, where historical credit card transaction data are obtained from the Kaggle repository. The collected dataset contains transaction records with anonymized features, transaction amount, transaction time, and class labels indicating whether each transaction is legitimate or fraudulent.

The second stage involves data preprocessing, which prepares the raw dataset for machine learning analysis. During this stage, duplicate transactions are removed, missing values are examined, numerical features are standardized using the StandardScaler technique, and the dataset is partitioned into training and testing subsets. These operations improve data consistency and reduce noise that could negatively affect model learning.

The third stage consists of feature engineering and class balancing. A new temporal feature representing the transaction hour is generated from the original time attribute to provide additional behavioural information. Subsequently, the Synthetic Minority Over-sampling Technique (SMOTE) is applied to the training dataset to generate synthetic fraud samples and balance the class distribution. This reduces bias toward legitimate transactions and improves the learning capability of the machine learning models.

The fourth stage focuses on machine learning model development. The balanced dataset is used to train multiple supervised learning algorithms capable of learning the underlying transaction patterns associated with fraudulent activities. The modular design of the framework allows different machine learning algorithms to be incorporated without modifying the overall system architecture.

The final stage performs fraud prediction and system evaluation. New financial transactions are processed through the trained models to determine whether they are legitimate or fraudulent. The modular structure of the framework also supports future deployment in intelligent financial monitoring systems capable of detecting suspicious transactions in near real-time.

Overall, the proposed framework establishes a comprehensive pipeline for transforming raw financial transaction data into reliable fraud predictions while ensuring flexibility, scalability, and reproducibility. The integration of preprocessing, feature engineering, and class balancing provides a strong foundation for developing accurate and robust financial fraud detection systems.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720044

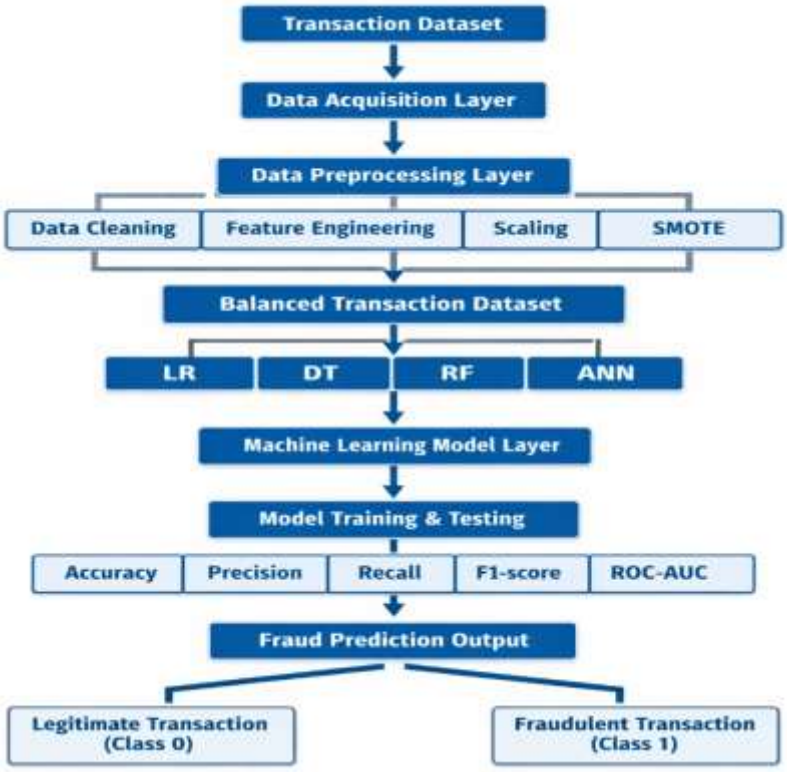

Figure 3.1: Proposed Machine Learning Framework for Financial Fraud Detection

Figure 3.1 illustrates the overall workflow of the proposed machine learning framework. The framework demonstrates the sequential processes involved in transforming raw financial transaction data into machine-learning-ready datasets before fraud prediction is performed.

Framework Validation

The proposed machine learning framework was successfully implemented and validated using the publicly available Kaggle credit card fraud dataset. The framework successfully completed all intended processing stages, including data acquisition, preprocessing, feature engineering, SMOTE-based class balancing, machine learning model development, fraud prediction, and performance evaluation. The successful execution of these stages demonstrates the feasibility, robustness, and scalability of the proposed framework for intelligent financial fraud detection.

3.7 Proposed System Architecture

The proposed system architecture was designed to implement the machine learning framework within a structured and modular environment suitable for financial fraud detection. The architecture consists of interconnected functional components that collectively perform data processing, model development, fraud prediction, and result generation. Each module performs a specific responsibility while interacting with other components through a well-defined processing pipeline.

The architecture begins with the data source layer, where historical credit card transaction records are collected from the Kaggle dataset. These records serve as the primary input to the fraud detection system.

The second layer is the preprocessing module, responsible for data cleaning, duplicate removal, feature scaling, and feature engineering. At this stage, the Hour feature is extracted from transaction timestamps, and the training dataset is balanced using SMOTE to improve the learning capability of subsequent machine learning models.

The processed data are forwarded to the machine learning module, where supervised learning algorithms are trained to recognize patterns associated

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720044

with fraudulent and legitimate transactions. The modular design enables multiple algorithms to be incorporated into the framework without affecting the remaining system components.

The prediction module receives unseen transaction data and generates fraud predictions based on the trained machine learning model. Each transaction is classified as either legitimate or fraudulent together with an associated prediction probability.

Finally, the output module displays the classification results and provides performance information that can assist financial institutions in identifying suspicious transactions for further investigation.

The proposed architecture follows a layered design that separates data management, preprocessing, machine learning, and prediction tasks. This modular organization improves maintainability, scalability, and future integration with real-time financial transaction monitoring systems.

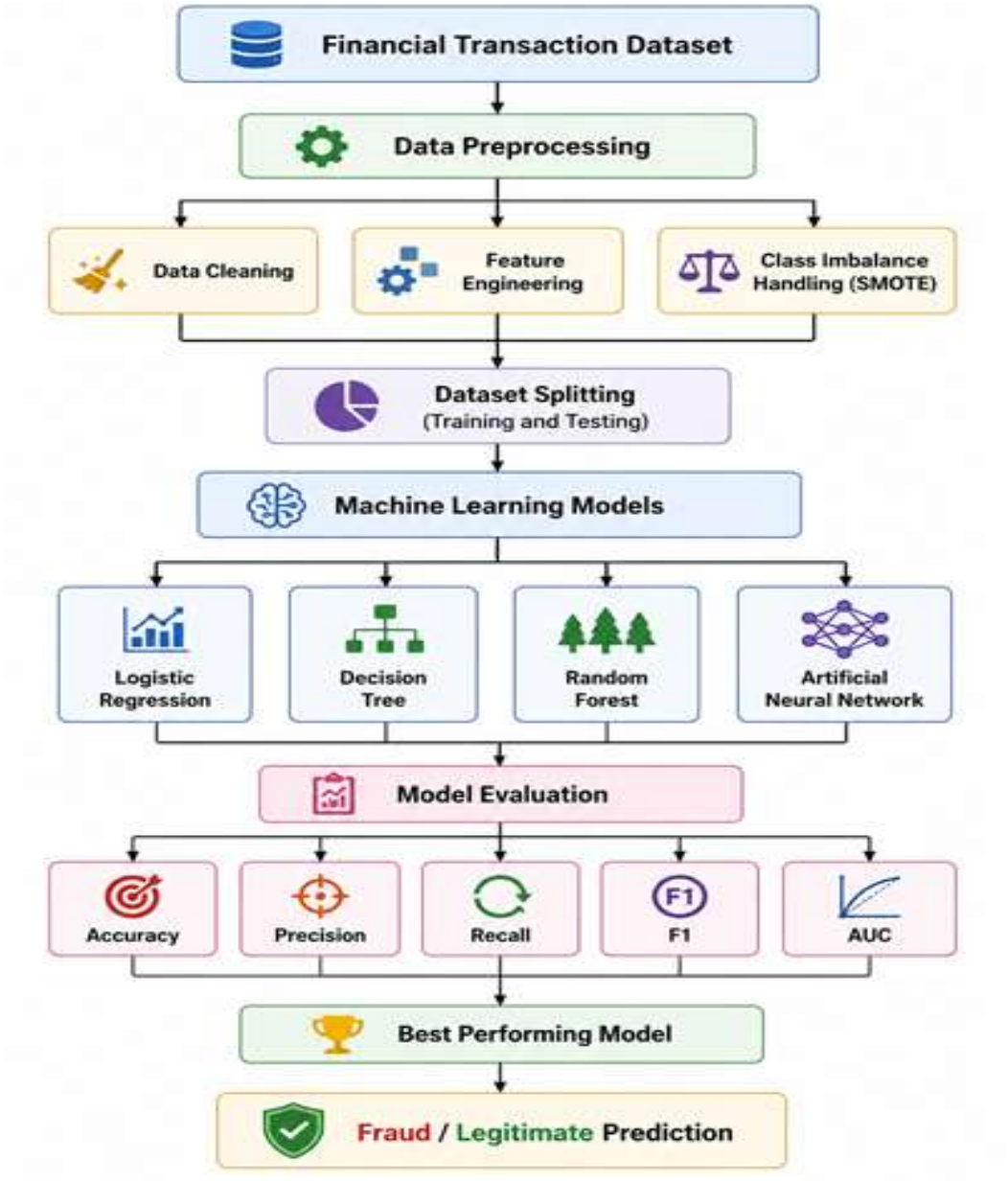

Figure 3.2: Architecture of the Proposed Financial Fraud Detection System

Figure 3.2 presents the architecture of the proposed financial fraud detection system. The architecture illustrates how transaction data flow through preprocessing, feature engineering, machine learning, prediction, and output modules to produce fraud detection decisions.

IV. DISCUSSION

The proposed machine learning framework provides a structured and practical approach for financial fraud detection by integrating data preprocessing, feature engineering, class balancing, and machine learning into a unified workflow. Unlike many existing studies that primarily focus on evaluating the predictive performance of classification algorithms, this research emphasizes the development of a comprehensive framework capable of supporting reliable fraud detection in real-world financial environments.

One of the major contributions of the proposed framework is the incorporation of comprehensive preprocessing techniques before model development. The framework includes duplicate removal, feature scaling, temporal feature engineering, and Synthetic Minority Over-sampling Technique (SMOTE) to improve data quality and address the severe class imbalance commonly encountered in financial transaction datasets. These preprocessing operations improve the representativeness of minority-class transactions and enhance the readiness of the dataset for machine learning applications. Similar observations have been reported in recent studies, which identified data preprocessing as a critical factor influencing fraud detection performance (Hernandez Aros et al., 2024).

Another significant contribution is the modular architecture of the framework. By separating data acquisition, preprocessing, feature engineering, model development, prediction, and evaluation into independent functional components, the framework provides flexibility for integrating different machine learning algorithms without modifying the overall system structure. This modular design improves maintainability, scalability, and adaptability for deployment in financial institutions where fraud detection requirements continuously evolve.

Compared with the benchmark study by Sadineni (2020), the proposed framework introduces several methodological improvements. While the benchmark research relied primarily on Principal Component Analysis (PCA) for feature representation and evaluated machine learning models using a limited set of performance metrics, the present framework incorporates SMOTE-based class balancing, engineered temporal features, and a structured preprocessing pipeline designed to improve model readiness. Furthermore, the framework establishes a modular system architecture that can be extended for future real-time financial fraud monitoring applications.

Recent developments in financial fraud detection have increasingly emphasized the importance of explainable, scalable, and deployable machine learning systems. Reviews published in 2025 and 2026 highlight that future fraud detection research should integrate robust preprocessing strategies with practical deployment frameworks to improve transparency, scalability, and operational effectiveness (Almalki & Masud, 2025; Thivaios et al., 2026).

Similarly, Almalki and Masud (2025) demonstrated that integrating explainable artificial intelligence with ensemble learning improves transparency and predictive performance in fraud detection. Unlike their approach, the present study emphasizes a comprehensive machine learning framework that integrates preprocessing, feature engineering, SMOTE-based class balancing, modular system architecture, and performance evaluation, thereby providing a broader methodological foundation for practical fraud detection systems.

The proposed framework aligns with these recommendations by providing a reproducible methodology that supports future integration with intelligent financial monitoring systems.

Overall, the proposed framework establishes a reliable methodological foundation for developing machine learning-based financial fraud detection systems. Its structured design enhances reproducibility, facilitates future model development, and provides a scalable architecture that can be adapted to evolving financial fraud detection requirements.

Table: 4 Dataset Structure

Attribute Category	Description
Time	Transaction timestamp
V1–V28	PCA-anonymized transaction features
Amount	Transaction amount
Class	Target variable (0 = Legitimate, 1 = Fraudulent)

V. CLASS DISTRIBUTION ANALYSIS

The dataset exhibited a severe class imbalance problem, which is common in fraud detection systems. Out of 284,807 transactions, only 492 transactions were fraudulent, while 284,315 transactions were legitimate.

Table 5: Original Class Distribution

Class	Number of Transactions	Percentage
Legitimate (0)	284,315	99.83%
Fraudulent (1)	492	0.17%
Total	284,807	100%

The results clearly show that fraudulent transactions represented only a very small portion of the dataset. This imbalance could significantly affect machine learning performance because models may become biased toward predicting legitimate transactions, leading to poor detection of minority fraudulent cases (He & Garcia, 2009).

VI. DATA PREPROCESSING RESULTS

Data preprocessing was performed before model training to improve data quality and ensure that the dataset was suitable for machine learning algorithms.

6.1 Duplicate Value Handling

The dataset was examined for duplicate values before model training. No missing values were detected in any of the attributes. However, 1,081 duplicate records were identified and removed during preprocessing, reducing the dataset size from 284,807 to 283,726 records. This ensured that the machine learning models were trained on unique transaction records.

Table 6: Duplicate Value Analysis

Description	Count
Original Dataset	284,807
Duplicate Records Removed	1,081
Dataset after Cleaning	283,726
Missing Values	0

The cleaning process improved dataset reliability and ensured that all machine learning algorithms operated on complete and consistent data.

6.2 Feature Engineering and Scaling

Feature engineering was successfully performed by generating an additional Hour attribute from the Time feature. This feature enabled the models to identify possible temporal fraud patterns associated with transaction timing.

Furthermore, RobustScaler normalization was applied to the Time and Amount attributes to reduce the influence of outliers. The PCA-transformed variables V1–V28 were already standardized and therefore required minimal additional scaling.

6.3 SMOTE Oversampling Results

To address the severe class imbalance problem, the Synthetic Minority Oversampling Technique (SMOTE) was applied to the training dataset.

Table 7: Class Distribution Before and After SMOTE (Training Dataset)

Training Dataset	Legitimate Transactions (Class 0)	Fraudulent Transactions (Class 1)	Total
Before SMOTE	198,277	331	198,608
After SMOTE	198,277	198,277	396,554

The Synthetic Minority Oversampling Technique (SMOTE) was applied only to the training dataset to address the severe class imbalance problem. Before applying SMOTE, the training dataset contained 198,277 legitimate transactions and 331 fraudulent transactions, indicating a severe class imbalance. After applying the Synthetic Minority Oversampling Technique (SMOTE), the minority class was oversampled to 198,277 fraudulent transactions, resulting in a balanced training dataset of 396,554 transactions. This balanced dataset was subsequently used to train the machine learning models, thereby reducing bias toward the majority class and improving the models' ability to detect fraudulent transactions.

6.4 Train-Test Partitioning

The dataset was partitioned into training and testing subsets using a 70:30 ratio, The 70:30 train-test split is a commonly adopted approach in supervised machine learning experiments because it provides sufficient data for model learning while maintaining an independent dataset for evaluation (Kotsiantis et al., 2007).

Table 8: Train-Test Split Results

Dataset	Number of Samples after duplicate remove	Percentage
Training Set	198,608	70%
Testing Set	85,118	30%
Total	283,726	100%

Stratified sampling ensured that the fraud-to-legitimate transaction ratio remained consistent in both subsets.

The proposed framework provides financial institutions with a structured methodology for developing intelligent fraud detection systems. Its modular architecture enables straightforward integration into banking platforms, fintech applications, and digital payment infrastructures. Furthermore, the incorporation of preprocessing, feature engineering, and SMOTE-based balancing improves data quality before model development, thereby enhancing the reliability of fraud detection systems operating in real-world financial environments

VII. CONCLUSION

This study presented a comprehensive machine learning framework for financial fraud detection using credit card transaction data. The framework integrates data acquisition, preprocessing, feature engineering, class balancing, model development, and fraud prediction into a unified and systematic workflow. By emphasizing data quality improvement through duplicate removal, feature scaling, engineered temporal features, and SMOTE-based class balancing, the framework establishes a robust foundation for developing intelligent fraud detection systems.

The proposed framework contributes to the field of financial fraud detection by providing a modular architecture that supports reproducibility, scalability, and future deployment in practical financial environments. Unlike many existing studies that primarily compare machine learning algorithms, this research focuses on establishing a structured methodology capable of improving dataset preparation and supporting reliable machine learning applications. The framework also addresses several limitations identified in previous studies by incorporating comprehensive preprocessing procedures and a flexible system architecture suitable for future extensions. Consequently, the proposed methodology provides a valuable foundation for researchers and practitioners seeking to develop efficient, scalable, and intelligent fraud detection systems.

Future research may extend he proposed framework by incorporating Explainable Artificial Intelligence (XAI), Graph Neural Networks (GNNs), federated learning, online learning algorithms, and streaming transaction analytics. Additionally, evaluating the framework using multiple financial datasets and real-time banking environments would further improve its practical applicability and generalizability.

REFERENCES

[1] Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

[2] Almalki, F., & Masud, M. (2025). *Financial fraud detection using explainable AI and stacking ensemble methods* (arXiv:2505.10050). arXiv. https://doi.org/10.48550/arXiv.2505.10050

[3] Ali, A., et al. (2022). *Financial fraud detection based on machine learning: A systematic literature review*. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637

[4] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[5] Bahnsen, A. C., Aouada, D., Ottersten, B., Stojanovic, J., & Diaz, C. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134–142. https://doi.org/10.1016/j.eswa.2015.12.030

[6] Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., & Oblé, F. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, 557, 317–331. http://dx.doi.org/10.1016/j.ins.2019.05.042

[7] Chawla, N. V., et al. (2002). *SMOTE: Synthetic minority over-sampling technique*. Journal of Artificial Intelligence Research, 16, 321–357.

[8] Chiaburu, T., Haußer, F., & Bießmann, F. (2024). Uncertainty in XAI: Human perception and modeling approaches. *Machine Learning and Knowledge Extraction, 6*(2), 1170–1192. https://doi.org/10.3390/make6020055

[9] Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2018). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications, 41*(10), 4915–4928.

[10] Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., et al. (2024). *Financial fraud detection through the application of machine learning techniques: A literature review*. Humanities and Social Sciences Communications, 11, Article 1130. https://doi.org/10.1057/s41599-024-03670-0

[11] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

[12] Preciado Martínez, P. M., López, A. M., & García, J. R. (2025). Comparative analysis of machine learning models for the detection of fraudulent banking transactions. *Cogent Business & Management, 12*(1), Article 2474209. https://doi.org/10.1080/23311975.2025.2474209

[13] Rao, R. K., & Mandhala, V. N. (2024). Unveiling financial fraud: A comprehensive review of machine learning and data mining techniques. *Informatica, 29*(6), 1–25. https://doi.org/10.18280/isi.290620

[14] Sadineni, P. K. (2020). *Detection of fraudulent transactions in credit card using machine learning algorithms*. Proceedings of the Fourth International Conference on I-SMAC (pp. 878–883). IEEE. https://doi.org/10.1109/I-SMAC49090.2020.9243545

[15] Shakeabubakor, A. A. (2024). Real-time fraud detection in financial transactions: An integrated approach using machine learning and cloud-based data warehousing. *International Journal of Intelligent Systems and Applications in Engineering, 12*(23s), 89–97. https://www.ijisae.org/index.php/IJISAE/article/view/7038

[16] 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

[17] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–56. https://doi.org/10.1016/j.cose.2015.10.005