Hybrid Adaptive Sampling With Risk-Based Credit Card Fraud Detection (HAS-RFD)

Mrs.M.Karthika[1], Rubhavashni LR[2], Muthamil E[3], Lavanya ShriR[4]
[1, 2, 3, 4] Dept of ComputerScience and Business Systems
[1, 2, 3, 4] K. Ramakrishnan College of Engineering, Trichy, India

Abstract- *Credit card fraud has become a significant challenge in the digital economy, resulting in substantial financial losses and reduced trust in online transactions. This paper presents a Hybrid Adaptive Sampling with Risk-Based Fraud Detection (HAS-RFD) framework integrated with Explainable Artificial Intelligence (XAI) techniques to improve fraud detection performance. The hybrid sampling method combines SMOTE-based oversampling with clustering-based adaptive undersampling to address class imbalance while preserving important data patterns. Machine learning models such as Random Forest and Logistic Regression are trained on the balanced dataset to classify transactions as fraudulent or legitimate. The system incorporates a risk-based classification mechanism that categorizes each transaction into Low, Medium, or High risk levels. Explainability techniques provide clear insights into fraud predictions, enhancing transparency and user trust. The proposed system achieves improved detection accuracy, reduced false positives, and enhanced interpretability, making it suitable for real- world financial applications.*

Keywords: Credit Card Fraud Detection, Hybrid Adaptive Sampling, SMOTE, Machine Learning, Explainable AI, Risk-Based Classification, Random Forest, Logistic Regression

I. INTRODUCTION

Background

The rapid growth of online financial transactions has made credit card fraud one of the most pressing challenges faced by banks, merchants, and cardholders worldwide. Fraudulent activities lead to significant financial losses and erode trust in digital payment systems. Traditional rule- based fraud detection systems struggle to keep pace with evolving fraud techniques, highlighting the urgent need for intelligent and adaptive solutions.

Machine learning has emerged as a powerful approach for detecting fraudulent transactions by learning patterns from historical data. However, a fundamental challenge in this domain is the highly imbalanced nature of fraud datasets, where genuine transactions vastly outnumber fraudulent ones, causing conventional models to be biased toward the
majority class.

Need for Intelligent Fraud Detection

Existing fraud detection systems often suffer from high false positive rates, where legitimate transactions are incorrectly flagged as fraudulent. Furthermore, many advanced models operate as black boxes, providing limited interpretability, which is a critical concern in financial decision-making environments.

Explainable Artificial Intelligence (XAI) has gained significant attention in financial applications as it allows models to communicate the reasoning behind their predictions. Integrating XAI with advanced sampling techniques can bridge the gap between model performance and user trust.

Scope of the System

The proposed HAS-RFD system can be deployed in banks, financial institutions, payment gateways, and e-commerce platforms. The platform supports real-time fraud detection, risk-based transaction classification, explainable model outputs, and user-friendly alert notification systems.

II. PROBLEM STATEMENT

With the rapid growth of online transactions, credit card fraud has become a major concern for financial institutions and customers. One of the primary challenges in fraud detection is the class imbalance problem, where fraudulent transactions represent only a small fraction of the total dataset. This imbalance causes traditional machine learning models to become biased toward legitimate transactions, resulting in poor fraud detection performance.

Existing fraud detection systems frequently exhibit high false positive rates and static sampling techniques that do not adapt to changing data distributions. The lack of interpretability in many advanced models further limits their acceptance in regulated financial environments. Therefore,

there is a need for an intelligent fraud detection system that can handle imbalanced data, provide accurate real-time predictions, reduce false positives, and offer clear explanations for its decisions.

III. OBJECTIVES

Main Objective

The main objective of this project is to develop a Hybrid Adaptive Sampling with Risk-Based Credit Card Fraud Detection (HAS-RFD) system that delivers improved detection accuracy, handles class imbalance effectively, and provides transparent and explainable fraud predictions.

Specific Objectives

The system aims to develop a hybrid adaptive sampling technique by combining SMOTE with clustering-based methods to handle class imbalance. It focuses on implementing machine learning models including Random Forest and Logistic Regression for accurate fraud classification. The system also incorporates a risk-based classification mechanism that assigns Low, Medium, or High risk scores to each transaction, and integrates Explainable AI techniques to enhance transparency and build user trust in model decisions.

IV. LITERATURE SURVEY

Several research studies have explored machine learning and AI applications for credit card fraud detection. Dal Pozzolo et al. (2017) presented a realistic modeling framework addressing key challenges including concept drift, class imbalance, and verification latency. Kilickaya (2019) evaluated multiple models on real credit card transaction data, finding that the Boosted Tree model achieved the best Fraud Detection Rate among Logistic Regression, Neural Networks, Random Forest, and SVM.

Ileberi et al. (2021) proposed a framework using SMOTE combined with AdaBoost on a European cardholder dataset, demonstrating improvements in accuracy, precision, recall, and AUC. Kilickaya (2023) further demonstrated that Random Forest with SMOTE outperforms Decision Trees for imbalanced fraud datasets. Recent work by Ahmed and Sagheer (2025) proposed an ensemble approach integrating SMOTE with Edited Nearest Neighbor (ENN) to combine noise removal with minority oversampling for improved model training.

V. PROPOSED SYSTEM

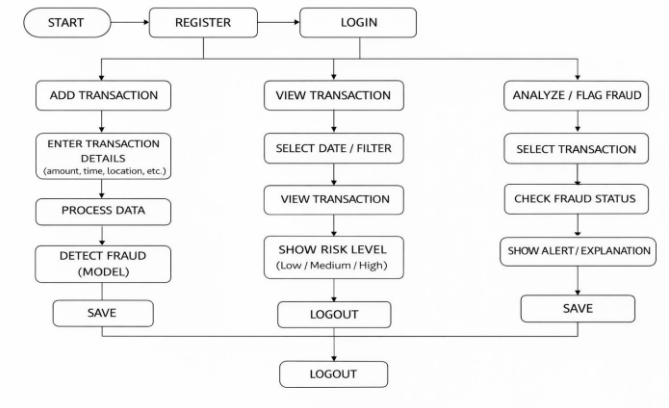
5.1 Overview

The proposed HAS-RFD system is an intelligent credit card fraud detection framework that combines hybrid adaptive sampling with risk-based classification and Explainable AI. The system is designed to accurately detect fraudulent transactions while providing interpretable results that build user trust and support financial decision-making.

5.2 Working Principle

Transaction data is first collected and preprocessed by handling missing values, removing noise, and normalizing features. The system applies a hybrid adaptive sampling technique combining SMOTE oversampling with clustering-based adaptive undersampling to balance the dataset. Trained machine learning models analyze transaction patterns and generate fraud predictions with probability scores. Based on these scores, transactions are categorized into Low, Medium, or High risk levels. The Explainable AI module then highlights key features contributing to each prediction, enabling users to understand the reasoning behind fraud alerts.

VI. SYSTEM ARCHITECTURE



The system architecture consists of three primary layers: the Presentation Layer, the Business Logic Layer, and the Data Layer. The Presentation Layer is the front-end interface developed using HTML, CSS, and JavaScript, enabling users to register, log in, add transactions, view transaction history, and access fraud detection results with risk classifications.

The Business Logic Layer is the core processing component where data preprocessing, hybrid adaptive sampling, machine learning model execution, risk-based

classification, and XAI analysis are performed. The Data Layer manages the secure storage and retrieval of user credentials, transaction records, and fraud detection results using SQLite or MySQL databases.

VII. METHODOLOGY

The proposed methodology begins with the collection and preprocessing of transaction data, where missing values are handled, noise is removed, and relevant features are selected. Data normalization is performed to improve model efficiency and ensure consistent input for further processing.

To address dataset imbalance, a hybrid adaptive sampling technique is applied by combining SMOTE with clustering methods, generating meaningful synthetic samples for the minority (fraud) class. The balanced data is then used to train Random Forest and Logistic Regression models. Transactions are classified into Low, Medium, and High risk levels, and Explainable AI techniques are incorporated to provide clear insights into model decisions.

VIII. HARDWARE IMPLEMENTATION

The hardware components required include a minimum of Intel Core i5 processor or equivalent, 16 GB RAM for handling large transaction datasets and concurrent processing, and 500 GB SSD storage for transaction data, user information, model outputs, and system logs.

A stable Gigabit Ethernet network connection is essential for reliable real-time fraud detection and alert generation. These hardware specifications ensure efficient execution of machine learning models and smooth system operation.

IX. SOFTWARE IMPLEMENTATION

The software implementation uses Python as the primary programming language due to its extensive library support for machine learning and data processing. The Flask framework is used as a lightweight web application backend. Machine learning libraries including Scikit-learn, Pandas, and NumPy are used for model training and analysis.

The frontend interface is developed using HTML, CSS, and JavaScript. SQLite is used as the database for storing user and transaction data. Authentication is managed using Flask-Login, and visualization is supported through Matplotlib for fraud trend analysis and performance metrics.

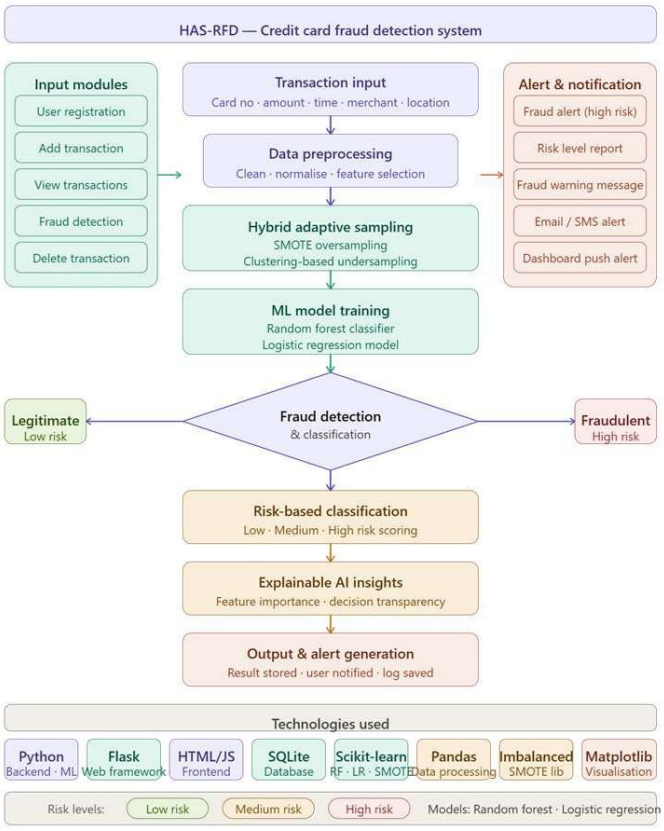


Fig. Software implementation — HAS-RFD credit card fraud detection system

X. RESULTS AND DISCUSSION

The proposed HAS-RFD system was tested across multiple transaction scenarios to evaluate its performance and reliability. The hybrid adaptive sampling technique effectively balanced the dataset, enabling the machine learning models to learn fraud patterns with significantly improved accuracy.

The system successfully classified transactions as fraudulent or legitimate and assigned appropriate risk levels based on prediction probabilities. The Explainable AI module provided clear and interpretable insights into the features driving each fraud prediction. Functionality, performance, and usability testing confirmed strong fraud detection capability with acceptable response times under normal operating conditions.

XI. ADVANTAGES

The proposed system addresses the class imbalance problem effectively through hybrid adaptive sampling, resulting in improved fraud detection accuracy and reduced false positives. Risk-based classification enables financial institutions to prioritize responses to suspicious transactions, improving operational efficiency.

The integration of Explainable AI enhances transparency and builds user trust by providing clear justifications for fraud detection decisions. The modular architecture ensures scalability, and the system is suitable for real-time deployment in diverse financial environments.

XII. APPLICATIONS

The HAS-RFD Credit Card Fraud Detection System can be deployed in banks, payment gateways, e-commerce platforms, insurance companies, and telecommunications companies for real-time fraud prevention and risk management. Its interpretable outputs make it especially suitable for regulated financial environments where model transparency is a critical requirement.

XIII. FUTURE ENHANCEMENTS

The system can be enhanced by incorporating advanced deep learning models such as Gradient Boosting and XGBoost to capture more complex fraud patterns. Real- time stream processing frameworks such as Apache Kafka or Spark Streaming can be integrated for instant transaction analysis.

Advanced XAI techniques including SHAP and LIME can be added to provide deeper feature-level explanations. Cloud deployment on AWS or Azure will improve scalability and global accessibility. Continuous learning capabilities will allow the model to adapt to evolving fraud techniques by retraining periodically on new transaction data.

XIV. CONCLUSION

The Hybrid Adaptive Sampling with Risk-Based Credit Card Fraud Detection (HAS-RFD) system provides an effective and intelligent solution for detecting fraudulent transactions in modern financial environments. By combining SMOTE-based oversampling with clustering- based adaptive sampling, the system addresses class imbalance and improves the learning capability of machine learning models.

The integration of Random Forest and Logistic Regression delivers accurate and reliable fraud predictions, while the risk-based classification mechanism enables informed decision-making. The inclusion of Explainable AI techniques provides transparent results that enhance user trust. The HAS-RFD framework is scalable, efficient, and suitable for real-world deployment, representing a significant contribution toward secure and intelligent digital financial transactions.

REFERENCES

[1] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines," International Journal of Computer Applications, 2011.

[2] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," IEEE Transactions on Neural Networks and Learning Systems, 2017.

[3] O. Kilickaya, "Predicting Credit Card Transaction Fraud Using Machine Learning Algorithms," International Journal of Advanced Computer Science and Applications, 2019.

[4] E. Ileberi, Y. Sun, and Z. Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost," IEEE Access, 2021.

[5] O. Kilickaya, "Credit Card Fraud Detection using SMOTE," Kaggle Research Repository, 2023.

[6] H. Ahmed and A. M. Sagheer, "Hybrid Sampling with Ensemble Learning for Credit Card Fraud Detection," Applied Soft Computing, 2025.

[7] N. Chawla et al., "SMOTE: Synthetic Minority Over-Sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321-357, 2002.

[8] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.

[9] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," in Advances in Neural Information Processing Systems (NIPS), 2017.

[10] M. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," in ACM SIGKDD, 2016