ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A Risk-Adaptive Temporal Transaction Intelligence Framework for Credit Card Fraud Detection and Explainable Financial Risk Assessment

[1]Koduri Sambasivarao, [2]Dr. K. Subba Reddy
[1]M. Tech Student, Department of CSE, Prakasam Engineering College (Autonomous), Kandukur, India
[2]Professor, Department of CSE, Prakasam Engineering College (Autonomous), Kandukur, India

ABSTRACT- ***Credit card fraud is a major challenge due to increasing digital transactions and changing fraudulent activities. Traditional methods struggle to identify suspicious patterns and handle imbalanced datasets. The proposed system uses Machine Learning and Deep Learning techniques to detect fraudulent transactions. SMOTE balances the dataset, while Random Forest selects the top 15 important features. StandardScaler normalizes the selected features. Algorithms such as Isolation Forest, One-Class SVM, Local Outlier Factor (LOF), and Autoencoder identify unusual transaction patterns. The best model is automatically selected using the Silhouette Score. The system supports fraud prediction and financial risk assessment by classifying transactions into Low, Medium, and High risk levels.***

KEYWORDS: - Credit Card Fraud Detection, Machine Learning, SMOTE, Anomaly Detection, Financial Risk Assessment.

INTRODUCTION

The increasing use of digital payments and online transactions has led to a rise in credit card fraud. Traditional rule-based systems often struggle to identify new fraudulent patterns and handle large transaction volumes. The proposed system uses Machine Learning and Deep Learning techniques to detect suspicious transactions effectively. SMOTE is applied to handle imbalanced data, while Random Forest selects the top 15 important features. Algorithms such as Isolation Forest, One-Class SVM, Local Outlier Factor (LOF), and Autoencoder identify unusual transaction patterns. The system automatically selects the best model using the Silhouette Score and supports financial risk assessment by classifying transactions into Low, Medium, and High risk levels.

RELATED WORK

Previous credit card fraud detection systems mainly used rule-based techniques and traditional Machine Learning algorithms such as Decision Trees, Logistic Regression, and Random Forest. These methods identify fraudulent transactions using predefined conditions and historical transaction patterns. However, they face challenges in handling highly imbalanced datasets and detecting previously unseen fraud activities. Recent anomaly detection approaches help identify unusual transaction behaviour by analysing patterns in financial data. The proposed framework combines SMOTE, Random Forest feature selection, Isolation Forest, One-Class SVM, Local Outlier Factor, and Autoencoder to improve anomaly detection and support financial risk assessment.

LITERATURE SURVEY

Existing studies on credit card fraud detection mainly focus on Machine Learning techniques such as Decision Trees, Logistic Regression, and Random Forest. These methods analyse transaction patterns to identify fraudulent activities. Some approaches use anomaly detection techniques such as Isolation Forest, One-Class SVM, and Local Outlier Factor to identify unusual transactions. Deep Learning methods like Autoencoders are also used to detect abnormal patterns through reconstruction errors. However, class imbalance and changing fraud behaviour remain major challenges. The proposed framework combines SMOTE, Random Forest feature selection, and multiple anomaly detection algorithms to improve fraud detection and support financial risk assessment.

EXISTING METHOD

The existing method uses rule-based systems and traditional Machine Learning algorithms such as Decision Trees, Logistic Regression, and Random Forest for credit card fraud detection. It analyses transaction data and identifies fraudulent activities based on predefined conditions and historical patterns. However, these methods face challenges in handling imbalanced datasets, detecting unknown fraud patterns, and adapting to changing fraudulent behaviors.

PROPOSED METHOD

The proposed method uses Machine Learning and Deep Learning techniques to improve credit card fraud detection and financial risk assessment. Initially, the credit card transaction dataset is loaded and analysed to understand the distribution of legitimate and fraudulent transactions. SMOTE is applied to handle class imbalance by generating synthetic minority samples. Random Forest is used to identify the top 15 important transaction features, reducing unnecessary data dimensions, while StandardScaler normalizes the selected features for consistent processing. The processed data is

analysed using different anomaly detection algorithms, including Isolation Forest, One-Class SVM, Local Outlier Factor (LOF), and Autoencoder, to identify unusual transaction patterns. Each model is evaluated using the Silhouette Score, and the highest-scoring model is automatically selected. The selected model, scaler, and important features are saved as separate Pickle files (model.pkl, scaler.pkl, and features.pkl) for future predictions. Finally, the system detects suspicious transactions and classifies financial risk into Low, Medium, and High levels, providing an intelligent approach to credit card fraud monitoring.

SYSTEM ARCHITECTURE

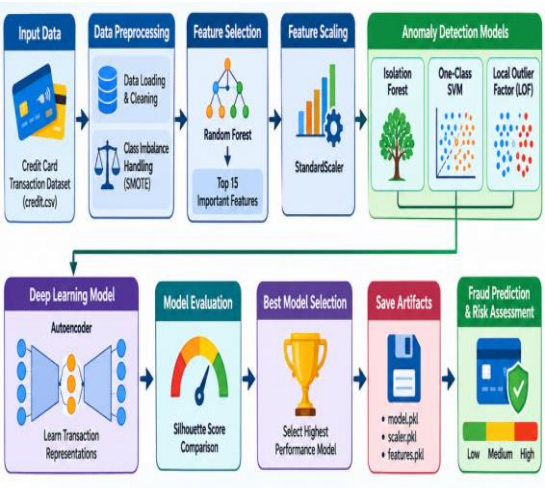

Fig. 1: Architecture of the Proposed Credit Card Fraud Detection and Risk Assessment System

The proposed architecture processes credit card transactions through data preprocessing using SMOTE, Random Forest feature selection, and StandardScaler. Isolation Forest, One-Class SVM, LOF, and Autoencoder detect unusual patterns. The best model is selected using the Silhouette Score and saved using Pickle for fraud prediction and Low, Medium, and High risk assessment.

METHODOLOGY DESCRIPTION

Data Ingestion Module: The data ingestion module is responsible for loading the credit card transaction dataset (credit.csv) into the system. It collects transaction records and analyses the available features to identify legitimate and fraudulent transactions. The loaded data is examined to understand its structure, size, and class distribution. This module provides the input data required for further preprocessing, feature selection, model training, and fraud detection.

Data Preprocessing Module: The data preprocessing module prepares the credit card transaction dataset for accurate fraud detection. SMOTE (Synthetic Minority Over-sampling Technique) is applied to handle class imbalance by generating synthetic samples for fraudulent transactions. Random Forest feature importance is used to select the top 15 important features, reducing unnecessary attributes. Finally, StandardScaler is applied to normalize the

selected features, ensuring consistent data input for the anomaly detection algorithms.

Exploratory Data Analysis Module: The Exploratory Data Analysis (EDA) module examines the credit card transaction dataset to understand its structure, patterns, and distribution. It analyses the number of legitimate and fraudulent transactions and identifies class imbalance in the dataset. The module helps understand transaction features and their importance, providing useful insights for feature selection, preprocessing, and further model development.

Model Building and Training Module: The model building and training module uses Machine Learning and Deep Learning algorithms to identify fraudulent credit card transactions. The selected features are processed using Isolation Forest, One-Class SVM, and Local Outlier Factor (LOF) to detect unusual transaction patterns. An Autoencoder is also used to identify anomalies based on reconstruction errors. All models are evaluated using the Silhouette Score, and the model with the highest score is automatically selected for further fraud prediction and risk assessment.

Model Evaluation Module: The model evaluation module compares the performance of different anomaly detection algorithms using the Silhouette Score. It measures the separation and compactness of the detected groups to identify the most suitable model. Isolation Forest, One-Class SVM, LOF, and Autoencoder results are evaluated, and the model with the highest Silhouette Score is automatically selected. The selected model, scaler, and features are saved using Pickle for future fraud prediction and financial risk assessment.

Prediction and Reporting Module: The prediction and reporting module uses the selected trained model, scaler, and important features to analyse new credit card transactions. It identifies suspicious transaction patterns and generates fraud prediction results. Based on the prediction, the system classifies the financial risk into Low, Medium, and High levels. The results help users understand potential fraud activities and support better financial risk assessment.

Deployment and User Interface Module: This module provides a user-friendly interface for entering transaction details and viewing fraud prediction results. The saved model identifies suspicious transactions and displays Low, Medium, and High financial risk levels.

RESULTS AND DISCUSSION

The proposed credit card fraud detection system analyses transaction data using Machine Learning and Deep Learning techniques. SMOTE helps handle class imbalance, while Random Forest selects the top 15 important features. Isolation Forest, One-Class SVM, LOF, and Autoencoder

identify unusual transaction patterns. The models are compared using the Silhouette Score to automatically select the best-performing model. The selected model supports fraud prediction and classifies financial risk into Low, Medium, and High levels. The results demonstrate the framework's potential for intelligent fraud detection and financial risk assessment.

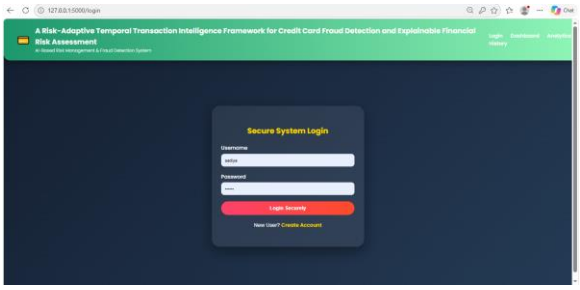

Fig. 2: Secure User Login Interface of the Proposed Credit Card Fraud Detection System.

The login page provides a secure interface for users to access the credit card fraud detection system. Users can enter their username and password to log in or create a new account. It also provides navigation to the Dashboard, Analytics, and Login History sections.

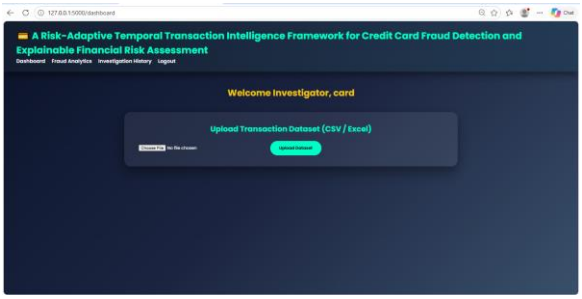

Figure 3: Credit Card Fraud Detection Dashboard

The dashboard allows investigators to upload transaction datasets in CSV or Excel format. It provides access to fraud analytics and investigation history for identifying and monitoring fraudulent transactions.

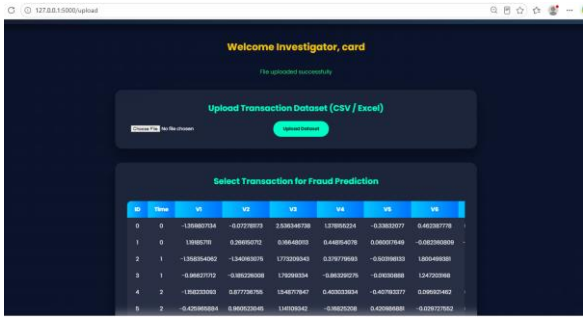

Figure 4: Transaction Dataset Upload and Preview

The uploaded transaction dataset is displayed in a tabular format with transaction IDs, time, and V1–V6 features. Investigators can review the dataset and select transactions for fraud prediction.

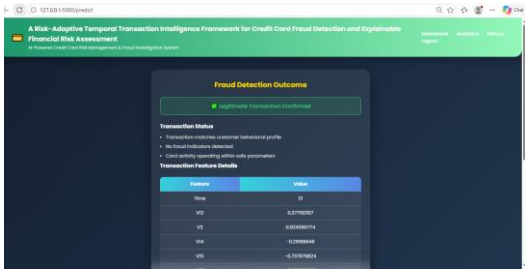

Figure 5: Credit Card Fraud Detection Prediction Result

The system analyzes the selected transaction and displays the fraud detection outcome. It confirms whether the transaction is legitimate based on transaction features and customer behavior patterns.

CONCLUSION

Risk-Adaptive Temporal Transaction Intelligence Framework provides an effective approach to credit card fraud detection and financial risk assessment. It combines machine learning and deep learning techniques to identify suspicious transaction patterns. SMOTE is used to handle imbalanced data, Random Forest selects important features, and anomaly detection algorithms identify unusual transactions. The best-performing model is selected using silhouette scores and saved for future predictions. Overall, this framework helps detect potentially fraudulent transactions and supports reliable financial risk assessment.

FUTURE SCOPE

In the future, the proposed system can be enhanced to detect fraudulent credit card transactions in real time. Explainable AI techniques can be integrated to provide clear reasons for identifying suspicious transactions. Temporal analysis can be used to understand transaction patterns over time and detect evolving fraud behaviours. The model can also be regularly updated with new transaction data to improve its performance. Advanced deep learning techniques can further improve fraud detection and financial risk assessment.

REFERENCES

1. Benchaji, I., et al. (2022). Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review. Link: https://doi.org/10.1016/j.jksuci.2022.11.008

2. Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost. Link:https://doi.org/10.1109/ACCESS.2021.3134330.

3. Lin, T. H., & Jiang, J. R. (2021). Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest. Link: https://doi.org/10.3390/math9212683

4. Du, H., Lv, L., Wang, H., & Guo, A. (2024). A Novel Method for Detecting Credit Card Fraud Problems. Link:https://doi.org/10.1371/journal.pone.0294537

5. Ngô, T. L., & Nguyễn, D. H. (2024). Detection of Credit Card Fraud Using a Deep Learning Autoencoder Model Combined with the Isolation Forest Algorithm. Link: https://doi.org/10.59276/JELB.2024.07CD.2761

6. Xie, Z., & Huang, X. (2024). A Credit Card Fraud Detection Method Based on Mahalanobis Distance Hybrid Sampling and Random Forest Algorithm. Link: https://doi.org/10.1109/ACCESS.2024.3421316

7. The Optimized Anomaly Detection Models Based on an Approach of Dealing with Imbalanced Dataset for Credit Card Fraud Detection (2022). Link: https://doi.org/10.1155/2022/8027903

8. Enhanced Credit Card Fraud Detection Based on SVM-Recursive Feature Elimination and Hyper-Parameters Optimization (2020). Link: https://doi.org/10.1016/j.jisa.2020.102596

9. Kennedy, R. K. L., Villanustre, F., & Khoshgoftaar, T. M. (2025). Unsupervised Feature Selection and Class Labeling for Credit Card Fraud. Link: https://doi.org/10.1186/s40537-025-01154-1

10. Wu, T., & Wang, Y. (2021). Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection. Link: https://arxiv.org/abs/2108.02501

11. A Systematic Review of Machine Learning in Credit Card Fraud Detection Under Original Class Imbalance (2025). Link: https://doi.org/10.3390/computers14100437

12. Enhanced Framework for Credit Card Fraud Detection Using Robust Feature Selection and a Stacking Ensemble Model Approach (2025). Link: https://doi.org/10.1016/j.rineng.2025.105084

13. Credit Card Fraud Detection Dataset – Machine Learning Group, ULB. Link: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

14. Scikit-learn Developers. Scikit-learn: Machine Learning in Python. Link: https://scikit-learn.org/stable/

15. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. Link: https://doi.org/10.1613/jair.953