International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 21-01-2026 Accepted: 26-02-2026 Published: 06-03-2026

ADVANCED FRAUD DETECTION IN E-COMMERCE USING MULTI-DIMENSIONAL USER BEHAVIOR ANALYTICS AND PROCESS MINING

Dr.S. Leela Krishna[1], P. Madhavi[2], S.Akhila[3], R.NalinKumar[4]
[1]Associate Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India
[2]Student, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India
[3]Student, Department of CSE,Teegala Krishna Reddy Engineering College, Hyderabad , India
[4]Student, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad , India
Email: , [1]leelakrishna46@gmail.com , [2]puttamadhavi17@gmail.com , [3]akhilasomishetty13@gmail.com, [4]nalinkumarrajula5@gmail.com

Abstract
Real-time fraud detection has become a crucial challenge for contemporary financial systems due to the exponential rise of digital financial transactions and the growing sophistication of cyber fraud schemes. Conventional fraud detection methods frequently find it difficult to adjust to dynamic and changing fraud trends because they are mostly dependent on rule-based frameworks and manual monitoring. These traditional methods are usually unable to detect complicated fraudulent actions due to high false-positive rates, restricted scalability, and slow reaction times. The combination of machine learning and artificial intelligence has become a viable approach to intelligent fraud detection in order to overcome these constraints. Large amounts of historical transaction data can be used by AI-driven algorithms to learn complex patterns and spot minute irregularities that might point to fraud. In order to examine real-time transaction data, this paper suggests an AI-based fraud detection system that makes use of machine learning methods, such as Support Vector Machines (SVM) and Decision Tree classifiers. The suggested solution employs predictive modeling and automated data analysis to identify unusual transaction trends. The framework greatly increases detection accuracy while lowering false positives and operating delays by facilitating real-time monitoring and quick decision-making. In addition, the technology improves flexibility and scalability in ever-changing financial contexts. Results from experiments show that the suggested method offers a reliable, effective, and scalable way to identify financial fraud, reducing losses and enhancing security in the quickly changing digital economy.

1 Introduction

The simplicity and effectiveness of financial services have been greatly enhanced by the growing reliance on online financial transactions in the quickly growing digital economy. But this expansion has also made fraud more likely, especially in the banking and e-commerce sectors. In addition to causing significant financial losses, fraudulent transactions erode user confidence in digital financial systems. Traditional fraud detection systems frequently fail to recognize intricate and dynamic fraud patterns in real time since they mainly rely on manual monitoring and static rule-based procedures. These drawbacks emphasize how urgently scalable, automated, and intelligent fraud detection systems are needed.

This project suggests a web-based system for detecting financial fraud that was created with the Django framework and combined with sophisticated machine learning methods, such as Random Forest classifiers and Support Vector Machines (SVM). Through data-driven predictive modeling, the system is intended to examine transaction statistics and identify questionable activity. Through an interactive web interface, users can submit transaction data, and the system will successfully discover possible fraud trends by performing data

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 21-01-2026 Accepted: 26-02-2026 Published: 06-03-2026

preprocessing, feature extraction, and model training.

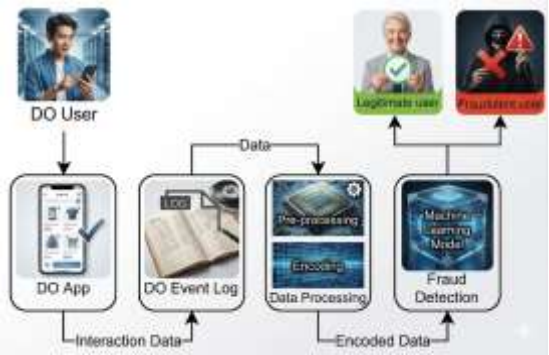

Figure 1 Applications

In order to guarantee accurate and transparent fraud detection results, the suggested platform additionally offers thorough model evaluation utilizing performance metrics including accuracy, precision, recall, and F1-score. Interactive data visualization tools are also included to give users a better understanding of transaction trends and anomalies. Better traceability and understanding of fraud-related behaviors are made possible by the system's integration of process mining tools for transaction workflow analysis.

The goal of this project is to create a scalable and adaptable fraud detection framework that can function in real-time settings, driven by the growing complexity of cyber fraud tactics and the shortcomings of traditional detection methods. The suggested approach can be used in a variety of industries, such as government financial systems, e-commerce, banking, and insurance. The technology helps to lower financial losses, improve security, and boost confidence in digital financial ecosystems by utilizing machine learning and intelligent data analysis.

2. Literature Survey

The act of acquiring financial gains through unlawful or dishonest means is known as financial fraud, and it frequently happens in industries like corporate finance, banking, insurance, and taxation. Money laundering and financial transaction fraud have grown to be significant issues for businesses and financial institutions in recent years. These dishonest practices have a detrimental impact on society and the world economy, resulting in large financial losses. Traditional manual or rule-based methods were the mainstay of earlier fraud detection techniques. Even though these techniques offered a certain amount of security, they were frequently expensive, time-consuming, and less precise when handling big amounts of transaction data.

Researchers have been concentrating more on cutting-edge methods like data mining, machine learning, and artificial intelligence (AI) for financial fraud detection in order to overcome these constraints. Systems can examine huge datasets and find hidden patterns that can point to fraudulent activity according to machine learning techniques. Fraud detection algorithms have used both supervised and unsupervised learning methods. Because they can learn from labeled datasets that contain feature vectors and class labels, classification algorithms are among the most popular. The model can identify new transactions as authentic or fraudulent after it has been trained. Nonetheless, a number of studies point out that the breadth of many current models is still constrained. Some research ignores crucial elements like evaluation procedures, comparative analysis, and the benefits and drawbacks of various data mining techniques in favor of concentrating mostly on prediction accuracy. As a result, more thorough methods are needed to enhance the dependability, effectiveness, and usefulness of financial fraud detection systems.

3.Methodology

Through the analysis of transactional data and past behavioral patterns, the suggested fraud detection framework incorporates cutting-edge machine learning algorithms to detect suspicious financial transactions. The system makes use of a well-known dataset, such the Credit Card Fraud Detection dataset on Kaggle, which includes comprehensive details on transactions, including timing, amount, merchant information, and other pertinent facts. A key element of the methodology is data preparation, which makes sure the dataset

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 21-01-2026 Accepted: 26-02-2026 Published: 06-03-2026

is clean and appropriate for machine learning analysis. In order to preserve consistency and boost model performance, missing or null values are eliminated, categorical properties are changed blabel encoding, and numerical features are normalized.

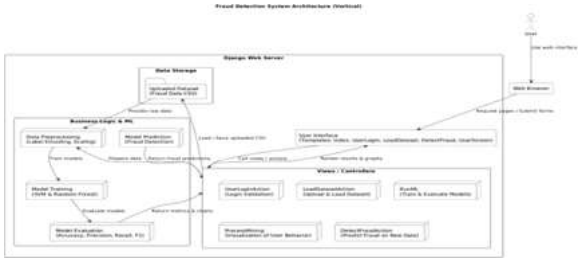

Figure 2: Proposed Block Diagram

The Support Vector Machine (SVM) is the initial classification model used in the suggested system. SVM is a potent supervised learning technique that finds the best hyperplane in a high-dimensional feature space to maximize differentiate fraudulent and legitimate transactions in order to conduct binary classification. The model can identify minor fraud trends that can be difficult to spot using traditional methods since kernel functions are used to capture complicated and non-linear interactions within the dataset. In order to enable the model to learn from past transaction data and assess its performance on previously unseen samples, the dataset is divided into training and testing subsets in an 80:20 ratio.

A Random Forest Classifier is also included to improve the system's resilience and predictive power. Random Forest is an ensemble learning technique that uses random feature selection and bootstrap sampling to build numerous decision trees. Features including transaction amount, device type, geographic location, transaction time, product category, and user account history are used to represent each transaction record. While the target variable (y_train) has binary labels indicating legal (0) or fraudulent (1) transactions, the training dataset (X_train) goes through preprocessing steps like normalization, encoding, and managing missing values.

The Random Forest technique creates a set of decision trees that independently assess various data subsets throughout the training stage. A majority voting process across all trees determines the final categorization, minimizing overfitting and lowering model variance. Following training, the model's predicted ability is evaluated using untested data (X_test). Performance measurements like accuracy, precision, recall, F1-score, and confusion matrix analysis are used to assess the efficacy of the suggested framework. These assessment metrics offer a thorough grasp of the model's capacity to identify fraudulent activity while reducing false positives, guaranteeing accurate and effective fraud detection in actual financial systems.

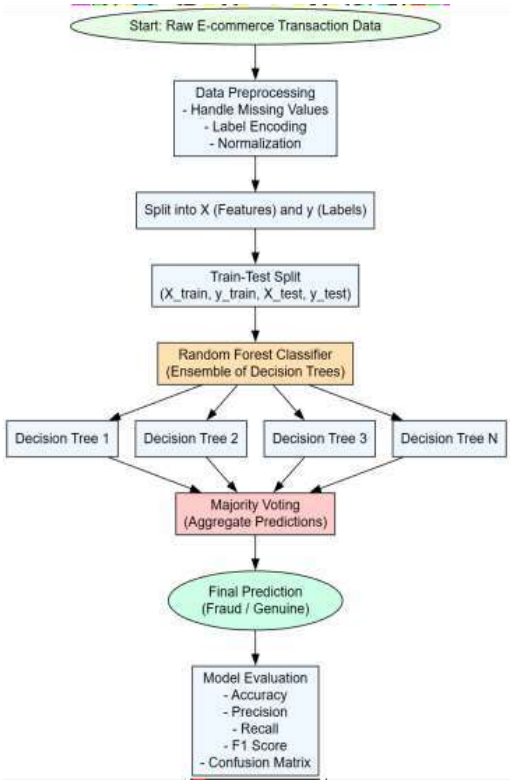

Figure 3: workflow of RFC

4 Results

The UI of the AI-based financial fraud detection web application, which is intended to guarantee usability, clarity, and effective financial transaction monitoring, is depicted in Figure 4. With the term "Financial Fraud Detection" prominently displayed at the top, the application's well-organized interface makes it easy to understand the goal of the system. Navigation choices like "Home" and "User Login" make it simple for users to

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 21-01-2026 Accepted: 26-02-2026 Published: 06-03-2026

access the platform's various modules. Secure access to user-specific dashboards and system features is guaranteed by the login-based authentication mechanism. Following authentication, customers can take advantage of the real-time transaction monitoring feature, which uses AI-based algorithms to continuously evaluate incoming financial data. These algorithms find suspicious transaction patterns and set off alarms for possible fraudulent activity by combining rule-based detection methods with behavioral analysis based on machine learning.

The system's login screen, shown in Figure 5, offers registered users a safe and intuitive authentication method. "Username" and "Password" are the two main input fields on the login form. While the password box is securely masked to protect critical information during entry, the username field enables users to submit their registered identity credentials. Users can submit their credentials for verification by clicking the prominently displayed "Login" button. Following a successful authentication process, users are granted access to the application dashboard, where they may carry out a number of tasks pertaining to fraud analysis, model training, and dataset administration.

Figure 4: Homepage

Figure 5: Login Page

The AI-based financial fraud detection system's main operating interface is shown in Figure 6. The interface's header, "AI-Based Financial Fraud Detection in Real-Time Transactions," reflects its organized and workflow-driven methodology. Several useful modules, like "Load & Process Dataset," "Process Mining," and "Run ML Algorithm," are included in the navigation panel and let the user navigate the whole analytical process. Users can upload transaction datasets using the "Browse Dataset" option in the "Load & Process Dataset" module. The system shows the file path for verification once a dataset file, like "fraud_transaction.csv," is chosen. Then, the "Submit" button starts the data loading and preprocessing necessary for model training and analysis.

Figure 6: Upload and processing the data

Following successful data loading, the dataset preview area is shown in Figure 7. Several transaction attributes, including transaction ID, fraud label, transaction value, and other anonymized details, are displayed in this section's structured view of the dataset. The dataset's abundance of columns suggests that it contains rich, high-dimensional data, which allows machine learning algorithms to identify a variety of patterns linked to fraudulent activity.

Figure 7: Pre-processed Data

The performance comparison between the suggested Random Forest Classifier (RFC)

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 21-01-2026 Accepted: 26-02-2026 Published: 06-03-2026

and the current Support Vector Machine (SVM) model is shown in Figure 8. The comparison shows that the suggested RFC model performs better in terms of classification and detection accuracy

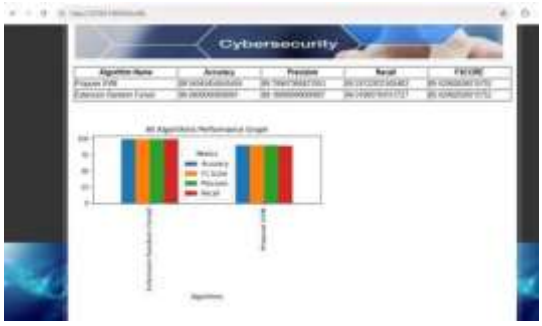

Figure 8: Comparison of Existing SVM and proposed RFC

when it comes to spotting fraudulent transactions. Compared to conventional classification models, the Random Forest algorithm's ensemble nature lowers the chance of overfitting and allows it to handle intricate data patterns.

Figure 9: upload Detect Fraud Dataset

The fraud detection system's interface for uploading and processing datasets is shown in Figure

9.

Figure 10: Predicted Outcomes

To assess the trained model, users can submit a different dataset using this module. To examine transaction patterns and identify questionable activity, the system combines machine learning and process mining approaches. Users can verify the efficacy of the fraud detection framework by testing the trained model on fresh datasets using the "Detect Fraud Module."

Lastly, the classification outcomes produced by the fraud detection model are displayed in Figure 10. To maintain secrecy and privacy, the dataset entries are either anonymized or encoded. The trained machine learning model examines each transaction record, and the resulting prediction is shown in the last column as either "Normal" or "Fraud." These findings show that the suggested system can reliably categorize transactions and identify fraudulent activity in huge financial datasets, promoting enhanced financial security and real-time fraud prevention.

5 Conclusion

The use of artificial intelligence (AI) in financial fraud detection has revolutionized how financial organizations spot and stop fraud. Even though they were helpful in the beginning, traditional rule-based systems frequently find it difficult to keep up with the ever-evolving and more complex tactics that fraudsters employ. On the other hand, AI-driven methods—especially those that rely on machine learning algorithms—offer a more flexible and perceptive framework for identifying fraudulent activity. Large amounts of transactional data may be analyzed in real time by these systems, which can also spot anomalies, irregular activity, and hidden patterns that might point to possible fraud. Financial institutions can lower the amount of false positives and greatly increase the accuracy of fraud detection by utilizing machine learning models. By reducing needless transaction disruptions, this improves the entire client experience and results in more effective operational procedures. The global market for AI-based fraud detection is anticipated to expand quickly in the upcoming years, reflecting the increasing use of AI technology in this field. This expansion demonstrates how financial institutions are depending more and more on intelligent solutions to safeguard digital financial

ecosystems.

AI-based fraud detection solutions also offer a number of benefits, such as scalability, real-time monitoring, and the capacity to continually learn from past transaction data. Without requiring a lot of user interaction, these features allow the system to adjust to changing fraud trends and evolving cyberthreats. But even with these benefits, there are still some difficulties. To guarantee the appropriate and moral application of AI technology, issues including data privacy concerns, the need for sizable and superior training datasets, and the possibility of algorithmic bias must be properly addressed. In conclusion, artificial intelligence (AI) has become a potent and successful tool for thwarting financial fraud in contemporary digital settings. The importance of sophisticated fraud detection systems will grow as the number and complexity of financial transactions continue to rise. Financial institutions may increase trust in digital financial services, lower financial losses, and fortify their security frameworks by incorporating AI-driven solutions.

References

[1].Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances, *Expert Systems with Applications*, vol. 193, pp. 116429, 2021; W. Hilal, S. A. Gadsden, and J. Yawney.

[2] *IEEE Access*, vol. 10, pp. 72504–72525, 2021; M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review."

[3] M. Albashrawi, “A Decade Review from 2004 to 2015: Detecting Financial Fraud Using Data Mining Techniques,” *Journal of Data Science*, vol. 14, pp. 553–570, 2016.

[4] In *Security and Communication Networks*, volume 2018, pp. 1–15, D. Choi and K. Lee, "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation."

[5] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "A Classification Framework and Academic Review of Literature on the Application of Data Mining Techniques in Financial Fraud Detection," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, 2021.

[6] *Engineering Applications of Artificial Intelligence*, vol. 76, pp. 130–157, 2019; N. F. Ryman-Tubb, P. Krause, and W. Garn, "How Artificial Intelligence and Machine Learning Research Impacts Payment Card Fraud Detection: A Survey and Industry Benchmark."

[7] "A Comprehensive Review from 2009 to 2019 on Financial Fraud Detection Using Data Mining Techniques," *Computer Science Review*, vol. 40, pp. 100402, 2021; K. G. Al-Hashedi and P. Magalingam.

[8] On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis via Interpretable Autoencoders, by J. Chaquet-Ulldemolins, S. Moral-Rubio, and S. Muñoz-Romero, *Applied Sciences*, vol. 12, no. 8, pp. 3856, 2022.

[9] *Artificial Intelligence Review*, vol. 53, pp. 2709–2748, 2019; A. Da’u and N. Salim, “Recommendation System Based on Deep Learning Methods: A Systematic Review and New Directions”.

[10] *Applied Sciences*, vol. 11, pp. 5656, 2021; Y. Zeng and J. Tang, "RLC-GNN: An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection."

[11] "Credit Card Fraud and Detection Techniques: A Review," *Banks and Bank Systems*, vol. 4, pp. 57–68, 2019, L. Delamaire, A. Hussein, and P. John.

[12] In *IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews*, volume 34, pages 513–522, 2021, D. Zhang and L. Zhou discuss "Discovering Golden Nuggets: Data Mining in Financial Applications."

[14] In *Proceedings of the International Conference on Computer, Communication and Electrical Technology (ICCCET)*, Tirunelveli, India, pp. 152–156, 2021, S. B. E. Raj and A. A. Portia, "Analysis on Credit Card Fraud

Detection Methods."
[14] "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," *arXiv preprint*, arXiv:1009.6119, 2020, C. Phua, V. Lee, K. Smith, and R. Gayler.
[15] *Computers & Security*, vol. 57, pp. 47–66, 2019; J. West and M. Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review."