International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

REAL-TIME TRANSACTION FRAUD DETECTION USING MACHINE LEARNING

Ms.M.Kavya[1], Harsha Begum[2], D.Neha[3], V.V.V.Satyadri[4]
Department of Artificial Intelligence & Data Science, Vidya Jyothi Institute of technology, Hyderabad ,India

ABSTRACT
Fraud detection in financial transactions has become a critical requirement in modern banking and digital payment systems due to the rapid increase in online transactions. In this project we present a Machine Learning (ML)-based fraud detection system designed to automatically identify suspicious and unauthorized transactions by analysing historical and real-time data. The system utilizes advanced algorithms such as Isolation Forest, One-Class Support Vector Machine (OC-SVM), and clustering techniques (K-Means, DBSCAN) to learn patterns of legitimate user behaviour and detect unusual transaction activities such as abnormal spending or unauthorized access. Key attributes including transaction amount, timestamp, location, and user behaviour are considered for accurate prediction. A comprehensive Data pre-processing stage is implemented, which includes handling missing values, data normalization, and feature engineering to enhance model efficiency and performance. The system is integrated with a backend and database (MongoDB/MySQL) for storing and retrieving transaction data, and a frontend interface for displaying results. It supports Real-time transaction monitoring, where incoming transactions are analysed instantly and suspicious activities are flagged for further action. This approach reduces manual intervention, improves detection efficiency, and provides a scalable and reliable solution for enhancing financial security.

1.INTRODUCTION
In recent years, digital payment systems and online banking services have grown rapidly, making financial transactions faster and more convenient. However, this growth has also increased the risk of fraudulent transactions, unauthorized access, and cybercrime. Fraud in financial systems causes huge losses to banks, businesses, and customers, making fraud detection an important requirement in modern banking systems.

Traditional fraud detection methods mainly depend on manual verification and rule-based systems. These methods are often slow, less accurate, and unable to handle large volumes of real-time transaction data. Fraudsters continuously change their techniques, making it difficult for fixed rule-based systems to identify new fraud patterns effectively.

The project titled “Real-Time Transaction Fraud Detection Using Machine Learning” aims to solve this problem by using Machine Learning techniques to automatically detect suspicious financial transactions. Instead of relying only on predefined rules, the system learns normal transaction behaviour from historical data and identifies unusual activities that may indicate fraud.

The proposed system uses algorithms such as Isolation Forest, One-Class Support Vector Machine (OC-SVM), and clustering methods like K-Means and DBSCAN. These algorithms help in identifying abnormal spending behaviour, unusual transaction timing, unauthorized access from different locations, and suspicious account activities.

The system considers important transaction attributes such as transaction amount, transaction time, user location, frequency of transactions, and customer behaviour patterns. These features help improve the accuracy of fraud prediction and reduce false alarms.

One of the major advantages of this project is real-time transaction monitoring. As soon as a transaction occurs, the system analyses it instantly and decides whether it is legitimate or suspicious. If fraud is detected, the system flags the transaction for further verification, reducing financial loss and improving customer security.

DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

The project also includes data pre-processing techniques such as handling missing values, normalization, and feature engineering to improve model performance. A backend system with database support (MongoDB/MySQL) is used for storing transaction details, while a frontend interface helps in displaying alerts and transaction reports.

This project provides a scalable, efficient, and reliable fraud detection system that improves banking security and minimizes manual effort. As digital transactions continue to increase, such intelligent fraud detection systems will play an important role in financial protection.

2. Literature Survey

2.1 Introduction to Fraud Detection

Fraud detection is the process of identifying suspicious financial activities that differ from normal user behaviour. It plays a major role in banking, credit card systems, insurance, and online payment platforms. With the growth of digital transactions, automated fraud detection systems have become essential.

2.2 Traditional Rule-Based Systems

Early fraud detection systems were based on predefined rules such as transaction amount limits, unusual login attempts, and suspicious account activity. These systems were simple but failed to detect new fraud patterns and required continuous manual updates.

2.3 Statistical Approaches

Statistical methods such as regression analysis and probability models were introduced to improve fraud detection. These methods identify unusual transaction patterns based on historical transaction behaviour. However, they were limited when dealing with large and complex datasets.

2.4 Machine Learning-Based Detection

Machine Learning techniques improved fraud detection by automatically learning patterns from transaction data. Supervised and unsupervised learning models are used to classify transactions as normal or fraudulent. These methods are more accurate and adaptive compared to traditional systems.

2.5 Isolation Forest Algorithm

Isolation Forest is an anomaly detection algorithm that isolates unusual transactions by randomly selecting features and split values. Fraudulent transactions are easier to isolate because they differ significantly from normal transactions. It is fast and effective for large datasets.

2.6 One-Class Support Vector Machine (OC-SVM)

OC-SVM is used when fraud examples are limited. It learns only from normal transaction data and identifies transactions that deviate from normal patterns. This makes it useful for detecting unknown fraud types.

2.7 Clustering Techniques

Clustering methods such as K-Means and DBSCAN group similar transactions together. Transactions that do not belong to normal clusters are treated as suspicious. These methods are useful for identifying hidden fraud patterns without labelled data.

2.8 Real-Time Fraud Detection

Modern systems focus on real-time monitoring where transactions are analysed immediately after they occur. This reduces delay in fraud identification and prevents financial damage before completion of fraudulent transactions.

2.9 Challenges in Existing Systems

Despite advancements, fraud detection systems still face challenges such as:

- High false positive rates
- Class imbalance in fraud datasets
- Detection of new fraud techniques
- Real-time processing requirements
- Large-scale transaction handling

These challenges motivate the development of more efficient and intelligent fraud detection systems

DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

3. Existing System

The existing fraud detection systems in financial institutions mainly rely on traditional rule-based methods and manual verification processes. These systems are designed using predefined conditions such as transaction amount limits, unusual login attempts, multiple failed password attempts, and sudden location changes. If a transaction violates these predefined rules, it is marked as suspicious for further investigation.

Although rule-based systems are simple and easy to implement, they have several limitations. Fraudsters continuously develop new techniques to bypass fixed security rules. Since traditional systems depend only on already known fraud patterns, they often fail to detect new and unknown fraudulent activities. This reduces the overall effectiveness of fraud prevention.

Manual fraud verification is another commonly used approach in existing systems. In this method, suspicious transactions are reviewed by human analysts before action is taken. While manual checking can improve decision accuracy, it is very time-consuming and difficult to manage when the number of daily transactions is very high. This creates delays in fraud detection and increases the risk of financial loss.

Some systems use statistical analysis methods such as regression models and probability-based detection. These methods compare current transaction behaviour with historical patterns to identify unusual activities. However, these approaches are less effective when dealing with large-scale real-time transaction data and complex fraud patterns.

With the advancement of technology, machine learning-based fraud detection systems were introduced. Supervised learning models such as Decision Trees, Random Forest, and Logistic Regression were used to classify transactions as normal or fraudulent. These methods improved detection accuracy but required large amounts of labelled fraud data for training, which is often difficult to obtain.

Unsupervised learning methods such as clustering and anomaly detection were also used in some systems. These systems detect fraud by identifying unusual transaction patterns without requiring labelled data. However, many of these systems still face challenges such as high false positive rates, poor real-time performance, and difficulty in handling massive transaction volumes.

Another limitation of existing systems is delayed fraud detection. Many systems analyse transactions only after they are completed, which means fraudulent transactions may already cause financial damage before detection. This creates a need for real-time fraud monitoring systems.

Overall, existing systems have made significant improvements in fraud detection, but they still suffer from limitations such as dependence on fixed rules, slow manual verification, difficulty in detecting new fraud patterns, and poor scalability. These drawbacks highlight the need for a more intelligent, automated, and real-time fraud detection solution.

4. Proposed System

The proposed system, “Real-Time Transaction Fraud Detection Using Machine Learning,” aims to provide an intelligent and automated solution for detecting fraudulent financial transactions in real time. Unlike traditional rule-based systems, this approach uses machine learning algorithms to learn transaction behaviour patterns and identify suspicious activities automatically.

The system is designed to monitor transactions continuously and instantly detect unusual or unauthorized activities. It focuses on improving fraud detection accuracy while reducing manual intervention and false alarms. The main objective is to protect users and financial institutions from financial losses caused by fraud.

The proposed system uses advanced anomaly detection algorithms such as Isolation Forest and One-Class Support Vector Machine (OC-SVM). These algorithms learn the normal transaction behaviour of users and identify transactions that significantly deviate from these patterns. Since fraudulent transactions are rare and often different from normal transactions, anomaly detection is highly effective.

DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

Clustering techniques such as K-Means and DBSCAN are also used to group similar transactions together. Transactions that do not belong to normal clusters are treated as suspicious. This helps in identifying hidden fraud patterns that may not be visible using traditional methods.

The system considers several important transaction features such as transaction amount, timestamp, transaction location, user login behaviour, transaction frequency, and spending patterns. These features help improve prediction accuracy and make fraud detection more reliable.

Before training the models, a complete data pre-processing stage is performed. This includes handling missing values, removing duplicate data, normalization, and feature engineering. These steps improve model efficiency and ensure better performance during prediction.

The system is integrated with a backend server and database such as MongoDB or MySQL for storing transaction details and fraud alerts. A frontend interface is also developed to display transaction history, fraud detection results, and warning notifications for suspicious activities.

One of the major advantages of the proposed system is real-time transaction monitoring. As soon as a transaction is initiated, the system analyses it immediately and decides whether it is safe or suspicious. If fraud is detected, the transaction is flagged for verification or temporarily blocked for security purposes.

The proposed system is scalable, cost-effective, and suitable for modern banking systems, online payment platforms, and digital financial services. It improves fraud prevention, enhances customer trust, and provides a reliable solution for financial security.

In conclusion, the proposed system offers a smarter and faster approach to fraud detection by combining machine learning, anomaly detection, clustering, and real-time monitoring. It overcomes the limitations of traditional systems and provides a more efficient solution for protecting financial transactions.

5. System Architecture

5.1 Data Collection

Transaction data is collected from banking systems, payment gateways, and customer transaction history. Important attributes such as amount, time, location, device information, and user behaviour are included.

5.2 Data Pre-processing

The collected data is cleaned by handling missing values, removing duplicates, and normalizing values. Feature engineering is also performed to improve the quality of input data for machine learning models.

5.3 Model Training

Machine learning models such as Isolation Forest, One-Class SVM, K-Means, and DBSCAN are trained using historical transaction data to learn normal transaction behaviour.

5.4 Real-Time Transaction Monitoring

When a new transaction occurs, the system instantly compares it with learned patterns and checks whether it is normal or suspicious.

5.5 Fraud Detection and Alert Generation

If the transaction is detected as suspicious, the system generates an alert and flags the transaction for further verification by the bank or customer.

5.6 Database Management

MongoDB/MySQL is used to store customer transaction records, fraud alerts, and transaction history for future analysis.

5.7 Frontend Interface

A user-friendly frontend interface displays transaction status, suspicious activity alerts, and fraud reports for administrators and users.

DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

6. Results

6.1 Successful Fraud Detection

The system successfully identifies suspicious financial transactions by analysing user behaviour and transaction patterns. Fraudulent activities such as unusual spending and unauthorized access are detected effectively.

6.2 Accurate Real-Time Monitoring

The system provides real-time transaction monitoring where transactions are analysed instantly after initiation. This helps prevent financial loss before fraud is completed.

6.3 Improved Detection Accuracy

Using Isolation Forest, OC-SVM, and clustering techniques improves fraud detection accuracy compared to traditional rule-based systems.

6.4 Reduced False Positives

The system reduces false alarms by learning genuine user transaction behaviour, which improves customer experience and reduces unnecessary transaction blocking.

6.5 Efficient Database Integration

The backend integration with MongoDB/MySQL allows secure storage of transaction records, fraud alerts, and customer information.

6.6 Scalable Performance

The system performs efficiently even with large transaction volumes, making it suitable for banks and online payment platforms.

6.7 Limitations Observed

Some limitations include:
Reduced performance with incomplete datasets
False detection in unusual but genuine transactions
Requirement of regular model updates

6.8 Overall Outcome

The project successfully demonstrates an intelligent fraud detection system that improves financial security using machine learning and real-time monitoring.

7. Conclusion

7.1 Summary of the Project

The project “Real-Time Transaction Fraud Detection Using Machine Learning” successfully provides an automated and intelligent system for detecting fraudulent financial transactions using machine learning techniques.

7.2 Achievement of Objectives

The main objective of detecting suspicious transactions in real time has been achieved. The system accurately identifies fraud and improves financial security.

7.3 Effectiveness of the System

The system performs efficiently by analysing large transaction volumes quickly and reducing manual verification efforts.

7.4 Advantages of the Proposed Approach

The system is scalable, accurate, cost-effective, and capable of detecting new fraud patterns without relying only on fixed rules.

7.5 Limitations Identified

The system may face challenges with highly complex fraud patterns, incomplete datasets, and rare unusual genuine transactions.

7.6 Overall Conclusion

Machine learning-based fraud detection is a practical and powerful solution for modern financial security systems and helps reduce fraud risks significantly.

7.7 Practical Applications

The system can be used in banks, credit card systems, insurance companies, online payment platforms, and e-commerce websites.

DOI:10.46647/ijetms.2026.v10i03.002 ISSN: 2581-4621

7.8 Contribution of the Project

This project contributes to financial technology by improving fraud prevention and demonstrating real-time intelligent fraud monitoring.

7.9 Scope for Enhancement

Future improvements can include deep learning models, blockchain integration, and advanced user behaviour analytics for better fraud prevention.

REFERENCES

1. Dal Pozzolo, A., Caelen, O., Johnson, R. A., and Bontempi, G., "Calibrating Probability with Undersampling for Unbalanced Classification," IEEE Symposium Series on Computational Intelligence, 2015.
2. Bhattacharyya, S., Jha, S., Tharakunnel, K., and Westland, J. C., "Data Mining for Credit Card Fraud: A Comparative Study," Decision Support Systems, vol. 50, issue 3, 2011.
3. Phua, C., Lee, V., Smith, K., and Gayler, R., "A Comprehensive Survey of Data Mining-based Fraud Detection Research," Artificial Intelligence Review, 2010.
4. Sahin, Y., and Duman, E., "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines," International MultiConference of Engineers and Computer Scientists, 2011.
5. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., and Bontempi, G., "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark," Information Fusion, 2019.
6.PricewaterhouseCoopers. Encuesta Global de Crimen y Fraude Económico de PwC Colombia 2022-2023; PricewaterhouseCoopers: London, UK, 2022. [Google Scholar]
7. Reurink, A. Financial fraud: A literature review. J. Econ. Surv. 2018, 32, 1292-1325. [Google Scholar] [Cross Ref]
8. Ahmed, M.; Mahmood, A.N.; Islam, M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016, 55, 278-288. [Google Scholar] [Cross Ref]
9. Roseline,, J.F.; Naidu, G.; Samuthira Pandi, V.; Alamelu alias Rajasree, S.; Mageswari, D.N. Autonomous credit card fraud detection using machine learning approach. Comput. Electr. Eng. 2022, 102, 108132. [Google Scholar] [CrossRef]
10. Tingfei, H.; Guangquan, C.; Kuihua, H. Using variational auto encoding in credit card fraud detection. IEEE Access 2020, 8, 149841-149853. [Google Scholar] [Cross Ref]
11. Dantas, R.M.; Firdaus, R.; Jaleel, F.; Neves Mata, P.; Mata, M.N.; Li, G. Systemic acquired critique of credit card deception exposure through machine learning. J. Open Innov. Technol. Mark. Complex. 2022, 8, 192. [Google Scholar] [CrossRef]
12. Dal Pozzolo, A.; Caelen, O.; Le Borgne, Y.A.; Waterschoot, S.; Bontempi, G. Learned lessons in credit card fraud detection from a practitioner perspective. Expert Syst. Appl. 2022, 41, 4915-4928. [Google Scholar] [Cross Ref]
13. Makki, S.; Assaghir, Z.; Taher, Y.; Haque, R.; Hacid, M.S.; Zeineddine, H. An experimental study with imhalanced classification annnachas for credit card fraud dataction IEEE Arrace 2010.