IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fraud Detection In Bank Payments Using Machine Learning Technique

Mr. SANTOSH MANDAVE
Computer Lecture
Address: Morarji Desai Residential PU College Arjunagi Tq: Afzalpur Dist: Kalaburagi

Abstract: Fraud detection in bank payments using machine learning is a critical area of aimed at preventing financial losses and enhancing security. Traditional fraud detection methods, such as manual verification and rule-based systems, are often time-consuming, expensive, and prone to inaccuracies. Machine learning

Index Terms - Fraud**,** detection**,** bank**,** financial**,** rule-based systems**.**

I. INTRODUCTION

Fraud detection in bank payments using machine learning is a critical area of aimed at preventing financial losses and enhancing security. Traditional fraud detection methods, such as manual verification and rule-based systems, are often time-consuming, expensive, and prone to inaccuracies. Machine learning offers a more efficient approach by analyzing large volumes of transaction data to identify fraudulent patterns Fraud detection in bank payments using machine learning is a critical area of research aimed at preventing financial losses and enhancing security. Traditional fraud detection methods, such as manual verification and rule-based systems, are often time-consuming, expensive, and prone to inaccuracies. Machine learning offers a more efficient approach by analyzing large volumes of transaction data to identify fraudulent patterns

1.1. PROBLEM DEFINITION

- With the rapid growth of online banking and digital transactions, financial institutions are facing increasing challenges in identifying fraudulent payment activities.
- Fraudulent transactions often resemble genuine ones, making manual monitoring difficult, time-consuming, and error-prone. Traditional rule-based systems are not sufficient, as fraudsters constantly change their strategies to bypass them.
- The problem is to develop an automated fraud detection system that can accurately distinguish between legitimate and fraudulent banking payments by analysing transaction patterns.
- Using machine learning techniques, the system should be able to learn from historical transaction data, identify suspicious activities in real time, and minimize both false positives (legitimate transactions flagged as fraud) and false negatives (fraudulent transactions not detected).
- The ultimate goal is to improve the security, reliability, and trustworthiness of banking systems while ensuring smooth and secure

2. OBJECTIVES:

1. To design and develop a machine learning model that can detect fraudulent banking transactions with high accuracy.
2. To analyze and identify patterns in transaction data that differentiates between genuine and fraudulent payments.
3. To reduce false positives and false negatives in fraud detection for better reliability.
4. To implement a system capable of providing real-time alerts for suspicious transactions.

5. To enhance the security and trust of digital payment systems through intelligent fraud detection. Customer transactions.

3. EXISTING SYSTEM:

The current fraud detection methods used in many banks and financial institutions are mostly rule-based systems and manual verification methods.

- **Rule-Based Systems:**
  Transactions are flagged based on predefined rules (e.g., unusually high amount, transactions from different countries within a short time, exceeding daily limits).
  These systems are simple to implement but lack adaptability. Once fraudsters learn the rules, they easily bypass them.
- **Manual Verification:**
  In some cases, suspicious transactions are reviewed manually by banking staff.
  This approach is time-consuming, costly, and inefficient for large volumes of real-time transactions.
- **Limitations of Existing Systems:**
  Inability to detect new or evolving fraud patterns.
  High number of false positives, where genuine transactions are wrongly marked as fraud.

4. PROPOSED SYSTEM:

- **Automated Fraud Detection**
  Uses supervised learning models like Random Forest and XG Boost to classify transactions as fraudulent or legitimate.
  Implements anomaly detection techniques to flag suspicious activities.

- **Real-Time Monitoring**
  Integrates with banking systems to analyse transactions instantly. Uses streaming data platforms like Apache Kafka for continuous fraud detection.

- **Enhanced Accuracy with AI**
  Employs deep learning models such as Neural Networks for improved fraud detection. Utilizes feature engineering to extract meaningful transaction patterns.

- **Scalability & Adaptability**
  Can handle large volumes of transactions efficiently. Continuously updates fraud detection models based on new data.

5. METHODOLOGY USED:

The fraud detection system is developed using machine learning techniques that analyse historical transaction data and classify payments as fraudulent or legitimate. The methodology includes the following steps:

1. Data Collection

- Gather historical transaction data containing both fraudulent and non-fraudulent records.
- Features include transaction amount, time, location, payment method, customer id, device used

2. Data Pre-Processing

- Handling missing values and noisy data.
- Normalization/standardization of numerical features.
- Encoding categorical values (e.g., transaction type, payment mode).
- Balancing the dataset using techniques like smote to deal with class imbalance (fraud cases are much fewer than genuine ones).

3. Feature Selection / Extraction

- Identify significant features that influence fraud detection (e.g., frequency of transactions, unusual location, abnormal amount).
- Reduce dimensionality to improve accuracy and efficiency.

4. Model Selection & Training

- Several machine learning algorithms can be applied, such as:
- Logistic regression – for binary fraud classification.
- Decision tree – for rule-based fraud identification.
- Random forest – to improve accuracy by combining multiple decision trees.
- K-nearest neighbours (k-n n) – for similarity-based classification.
- Neural networks / deep learning – for complex non-linear fraud patterns.

5. Model Evaluation

- Performance is measured using metrics such as:
- Accuracy – overall correctness of predictions.
- Precision – proportion of detected frauds that are truly fraud.
- Recall (sensitivity) – proportion of actual frauds detected.
- F1-score – balance between precision and recall.
- Roc-auk curve – model's ability to separate fraud vs. non-fraud.

6. HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Requirements

1	Processor	Intel i5 or equivalent
2	RAM	8 GB
3	Storage	256 GB SSD
4	GPU	Optional for small datasets
5	Any Desktop or Laptop systems with high level configuration	

Software Requirements:

1	Operating System	Windows/Linux/macOS
2	Programming Languages	Python, R (optional)
3	Libraries	Scikit-learn, TensorFlow, PyTorch, Pandas, NumPy
4	Database	MySQL
5	Tools	Anaconda, Jupiter Notebook

1. Data collection module

- Collects transaction data from banking systems (mobile apps, atms, pos, online banking).Includes customer details, transaction amount, time, location, device information, and payment method.Ensures data privacy and encryption during transfer.

2. Data preprocessing module

- Cleans raw data by handling missing values, duplicate records, and inconsistencies.Normalizes and transforms features (e.g., transaction amount scaling, time format conversion).Encodes categorical variables like payment type or merchant category for ml models.

3. Feature engineering module

- Generates new features to highlight fraud patterns:Transaction frequency within a time window.Average transaction value for a customer.Geographical distance between current and past transactions.Stores these features in a feature store for real-time and batch use.

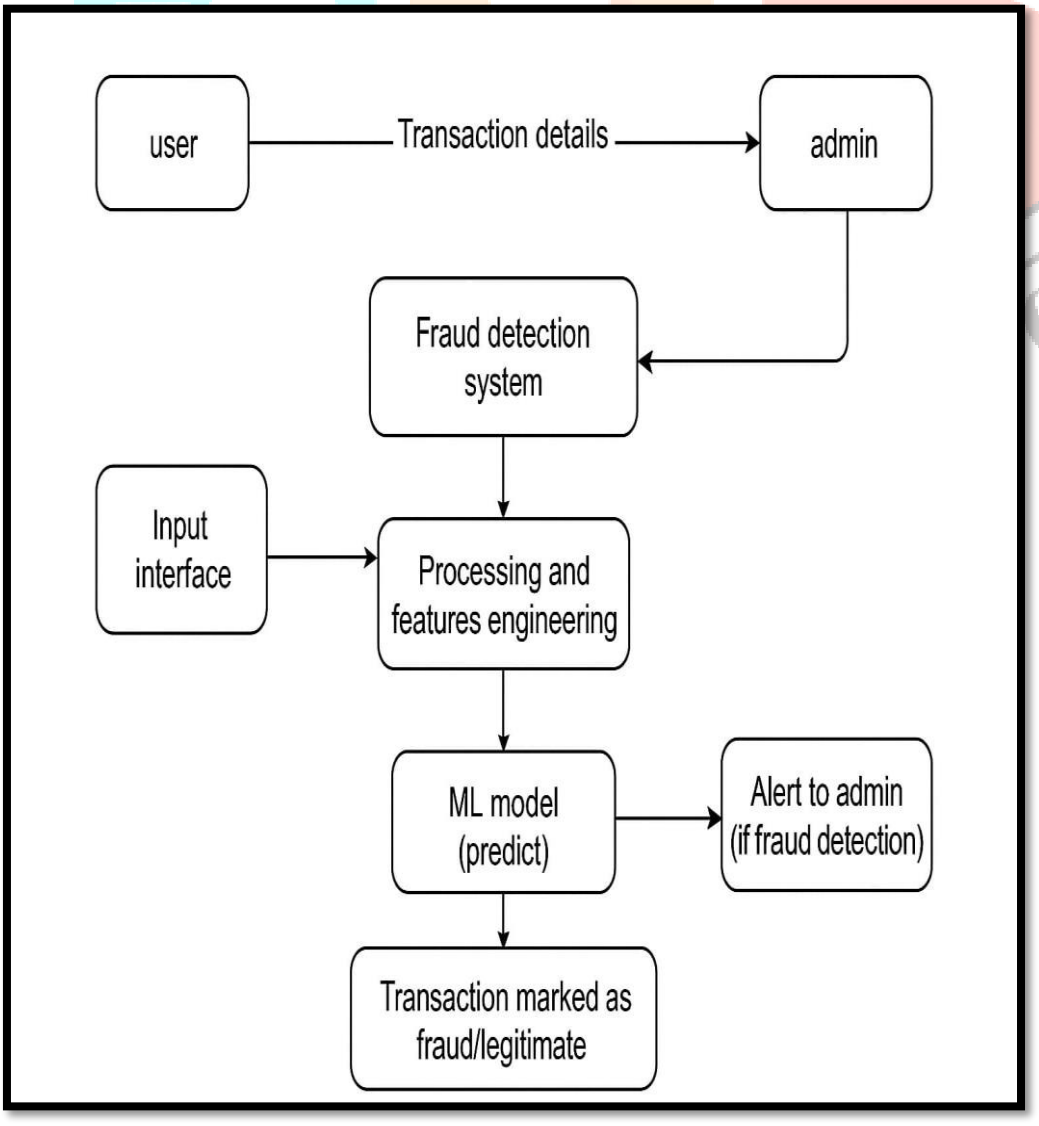
4. Model training module

- Uses historical labeled data (fraud / non-fraud).Applies machine learning algorithms such as logistic regression, random forest, or x g boost. Performs model evaluation using metrics like precision, recall, f1-score, and roc-auc.Selects the best-performing model for deployment.

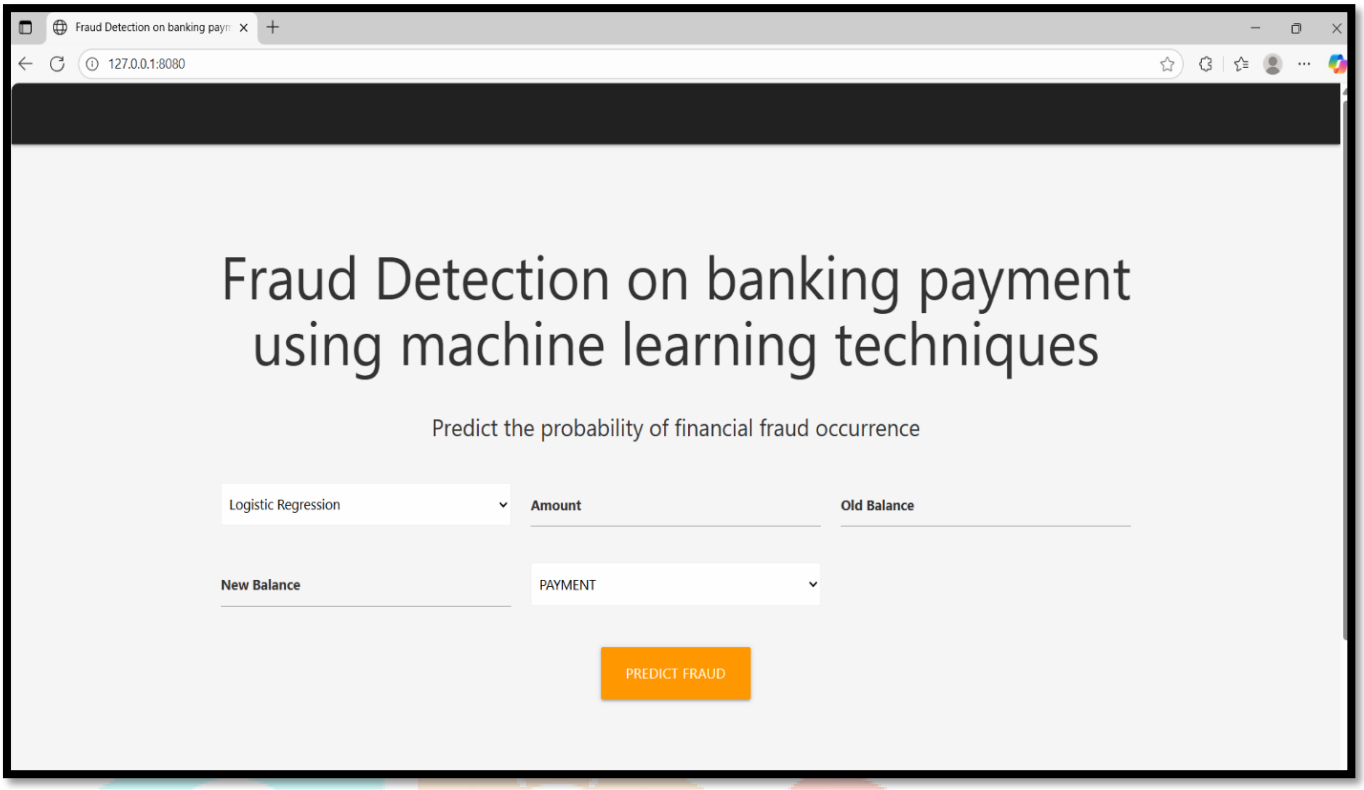
5. Fraud detection (inference) module

- Accepts live transaction requests. Retrieves features from the feature store. Predicts the probability of fraud using the trained ml model.

7. FLOW DIAGRAM



8. OUTPUT SCREEN



CONCLUSION

Machine Learning provides an efficient and automated approach to detect fraudulent banking transactions. Models can analyze large volumes of payment data in real-time and identify suspicious patterns. Helps in reducing financial losses, ensuring customer trust, and improving security. Continuous model training and updating are essential to adapt to new fraud techniques.

REFERENCES

[1] S. M. Darwish, "An intelligent credit card fraud detection approach based on semantic fusion of two classifiers," (in English), Soft Computing, Article vol. 24, no. 2, pp. 1243-1253, Jan 2020.

[2] A. Eshghi and M. Kargari, "Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty," (in English), Expert Systems with Applications, Article vol. 121, pp. 382-392, May 2019.

[3] S. Hossain, A. Abtahee, I. Kashem, M. M. Hoque, and I. H. Sarker, "Crime Prediction Using Spatio-Temporal Data," in Computing Science, Communication and Security, Singapore, 2020, pp. 277-289: Springer Singapore.

[4] M. Zamini and S. M. H. Hasheminejad, "A comprehensive survey of anomaly detection in banking, wireless sensor networks, social networks, and healthcare," (in English), Intelligent Decision Technologies-Netherlands, Article vol. 13, no. 2,pp. 229-270, 2019.

[5] I. Gonzalez-Carrasco, J. L. Jimenez-Marquez, J. L. Lopez-Cuadrado, and B. Ruiz-Mezcua, "Automatic detection of relationships between banking operations using machine learning," (in English), Information Sciences, Article vol. 485, pp. 319-346, Jun 2019.

Mr. SANTOSH MANDAVE
Computer Lecture
Address: Morarji Desai Residential PU College Arjunagi
Tq: Afzalpur Dist: Kalaburagi
E-mail- rchrsantosh@gmail.com