International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Online Payments Fraud Detection Using Machine Learning

K. Pujitha[1], G. Midun Surya Sai[2], J. Venkata Mohan[3], K. Brahma Rao[4], A. Leela Sai[5]
Dr. A. S. Kanaka Ratnam[6] | Professor, Department of CSE (AI & ML)
228x1a4236@khitguntur.ac.in[1], 228x1a4229@khitguntur.ac.in[2], 228x1a4231@khitguntur.ac.in[3], 228x1a4263@khitguntur.ac.in[4], 218x1a4250@khitguntur.ac.in[5], sriram.abburi@gmail.com[6]
Kallam Haranadhareddy Institute of Technology (Autonomous), Guntur, Andhra Pradesh, India

ABSTRACT:
The exponential growth of e-commerce has revolutionized global commerce, offering convenience and accessibility to consumers worldwide. However, this digital transformation has been accompanied by a surge in online payment fraud, posing a significant threat to businesses and consumers alike. Traditional rule based fraud detection systems are increasingly inadequate against sophisticated and evolving fraudulent techniques. Machine learning (ML) has emerged as a powerful paradigm shift in fraud detection, offering the ability to learn complex patterns, adapt to dynamic fraud landscapes, and proactively identify fraudulent transactions in real-time. This paper explores the critical role of machine learning in online payment fraud detection. It delves into the various machine learning techniques employed, including supervised, unsupervised, and deep learning approaches, highlighting their strengths and limitations. The paper further examines the essential data pre-processing steps, feature engineering strategies, and evaluation metrics crucial for building robust and effective fraud detection systems. Moreover, it discusses the challenges and future directions in this dynamic field, emphasizing the ongoing need for innovation to stay ahead of increasingly sophisticated fraudsters in the evolving digital payment ecosystem. Ultimately, this paper underscores the transformative potential of machine learning in safeguarding online transactions and fostering a more secure and trustworthy e-commerce environment

KEYWORDS:
Online Fraud, Payment Transactions, Multifaceted Approach Technology, Fraud Detection, Random Forest, Machine Learning

I. INTRODUCTION

In the digital age, online payments have become an integral part of everyday life, facilitating quick and easy transactions without the need for physical cash. This convenience, however, comes with the inherent risk of fraud. Fraudulent activities in online payments can lead to substantial financial losses and undermine trust in digital financial systems. Therefore, detecting and preventing online payment fraud is of paramount importance. This project explores the application of machine learning techniques to detect fraudulent transactions, aiming to enhance the security and reliability of online payment systems. Over the past few decades, the popularity of online payments has skyrocketed due to the ease of sending money from anywhere, a trend further fuelled by the COVID-19 pandemic. Studies indicate continued growth trajectory for e commerce and online payments in foreseeable future. However, this surge in online transactions has also led to an uptick in online payment fraud, necessitating heightened awareness among consumers and service providers. As online payment fraud has escalated in recent years, it's imperative for users to verify the legitimacy of their transactions to avoid potential repercussions such as reporting fraud, freezing payment methods, and risking exposure of personal data to criminals, which could lead to further criminal activity. On the flip side, companies must diligently scrutinize transactions to prevent unwittingly facilitating fraud and potentially having to reimburse clients to maintain their patronage, placing a strain on their resources. Despite companies' efforts to implement various fraud detection programs, only a fraction of them have proven effective in identifying online payment fraud. Fraudsters, adept at circumventing security measures, occasionally succeed in perpetrating online payment scams. Studies indicate a global increase in cumulative losses from fraudulent bank card transactions, underscoring the urgency of addressing this issue. Researchers have also focused on the concept of idea drift, wherein the underlying distribution of datasets evolves over time. Much like how consumer purchasing patterns change, fraudsters adapt their tactics accordingly. While fraudsters are constantly evolving, so too are professionals dedicated to uncovering and combatting these scams, which may lead to the obsolescence of certain fraudulent tactics over time.

Fraud, being an illegal means of obtaining something, necessitates the implementation of effective fraud detection systems (FDS) to monitor transactions and detect any suspicious activity. These systems employ machine learning and data mining techniques to analyse transaction patterns and distinguish between fraudulent and legitimate transactions. By analysing data patterns, a combination of these techniques can effectively identify fraudulent transactions and mitigate the risks associated with online payment fraud.

Fraud detection refers to the process of monitoring transactions and customer behaviour to pinpoint and fight fraudulent activity. It is usually a central part of a firm's loss prevention strategy and sometimes forms a part of its wider anti money laundering (AML) compliance processes.

II.LITERATURE SURVEY

S. No	Author / Year	Method Used	Key Findings	Limitations
1	Kulkarni (2019)	Random Forest, LOF	Effective in detecting credit card fraud using classification and anomaly detection	High false positives in imbalanced datasets
2	Nanda et al. (2018)	Rule-Based Systems	Simple and easy to implement fraud detection	Cannot adapt to new fraud patterns
3	Lalev (2019)	Deep Neural Networks (DNN)	High accuracy in detecting complex fraud patterns	Requires large training data
4	Papasavva et al. (2024)	AI-based Models	Improved fraud detection using AI techniques	Computationally expensive
5	Ukidve et al. (2017)	PCI DSS Compliance	Enhances payment security standards	Implementation complexity
6	Halsteinslid (2019)	Logistic Regression	Good for binary classification and interpretability	Less effective for complex datasets
7	Chen et al. (2024)	Deep Forest / Ensemble	Better performance using hybrid models	Increased model complexity
8	Lv et al. (2022)	Logistic-SVM Hybrid	Improved classification accuracy	Requires parameter tuning
9	Thimonier et al. (2023)	Anomaly Detection	Useful for detecting unknown fraud patterns	Sensitive to data imbalance
10	Ni et al. (2024)	Feature Boosting + Oversampling	Handles imbalanced datasets effectively	Higher computational cost
11	Fernandes (2013)	Fraud Analysis Study	Identified major fraud types and threats	Lacks implementation model
12	Rahman et al. (2017)	Real-time Fraud Prevention	Helps in early fraud detection	Difficult to scale
13	Yuan et al. (2017)	Deep Neural Networks	Accurate detection using deep learning	Needs high processing power
14	Sharma et al. (2023)	AI Automation	Automates fraud detection process	Requires continuous updates
15	Yue et al. (2025)	GAN-based Models	Detects deepfake fraud with high accuracy	Complex model training

The study of online payment fraud detection has gained significant attention due to the rapid growth of digital transactions. Various researchers have explored different techniques ranging from traditional rule-based systems to advanced machine learning and deep learning models.

Early fraud detection systems primarily relied on **rule-based approaches**, which use predefined conditions to identify suspicious activities. However, these methods are limited because they cannot adapt to evolving fraud patterns and often result in high false positives .

With the advancement of technology, **machine learning (ML) techniques** have become widely adopted for fraud detection. Algorithms such as Logistic Regression, Random Forest, Support Vector Machine (SVM), and Gradient Boosting have shown promising results in identifying fraudulent transactions. These models can learn patterns from historical data and improve detection accuracy over time

III.PROBLEM STATEMENT

- The rapid growth of online payment systems has increased the risk of fraudulent transactions.
- Traditional fraud detection methods are not effective in identifying modern and evolving fraud patterns.
- Fraudsters continuously develop new techniques to bypass existing security systems.
- Current systems often produce high false positives, affecting genuine users.
- Handling large volumes of transaction data in real-time is a major challenge.
- Many existing models fail to detect rare and complex fraud cases accurately.
- There is a need for intelligent systems that can learn from data and adapt over time.
- Ensuring both security and user convenience remains difficult.
- Lack of efficient feature selection reduces model performance.
- Therefore, an advanced machine learning-based fraud detection system is required to improve accuracy and reliability.

IV.PROPOSED SYSTEM

- The proposed system uses machine learning algorithms to detect fraudulent transactions.
- Transaction data is collected and preprocessed to remove missing and irrelevant values.
- Important features are selected to improve model performance and accuracy.
- Multiple models such as Logistic Regression, Random Forest, SVM, and XGBoost are implemented.
- Different models are compared to identify the best-performing one.
- An ensemble approach is used to improve detection accuracy and reduce false positives.
- The model is trained using historical transaction data to learn fraud patterns.
- Real-time transaction monitoring is applied to detect suspicious activities instantly.
- Evaluation metrics like accuracy, precision, recall, and ROC-AUC are used to measure performance.
- The system aims to provide a secure, reliable, and efficient solution for online payment fraud detection.

V.METHODOLOGY

1. Collect Data

Historical online payment transaction data is collected from datasets.
This data includes details like amount, time, user behavior, and transaction type.

2. Preprocess Data

The collected data is cleaned by removing missing or incorrect values.
Normalization and formatting are done to make the data suitable for model training.

3. Feature Selection

Important features that help in identifying fraud are selected.
This step improves accuracy and reduces unnecessary data processing.

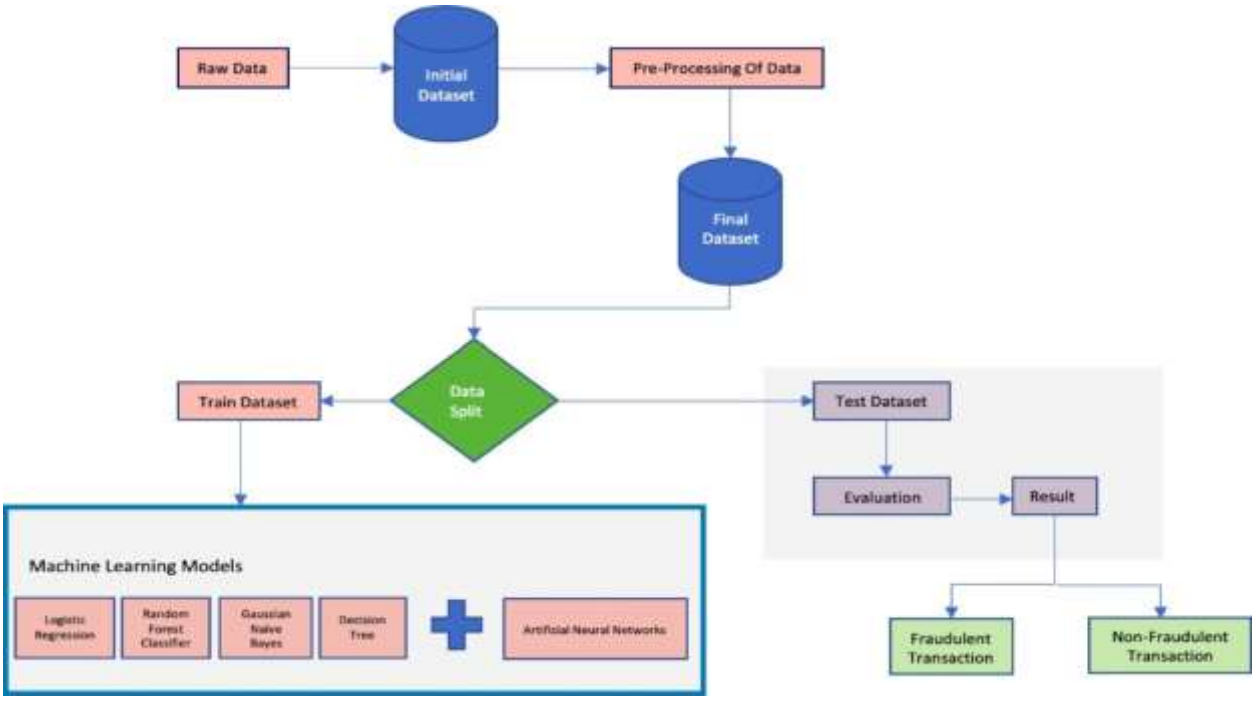
4. Train Model

Machine learning algorithms like **Random Forest** and **Logistic Regression** are used.
The model learns patterns from past transactions to identify fraud.

5. Predict Fraud

The trained model analyzes new transactions.
It classifies them as **fraudulent** or **legitimate** based on learned patterns.

VI. SYSTEM ARCHITECTURE



This architecture describes a complete end-to-end machine learning pipeline for classifying online payment transactions as fraudulent or legitimate. Here's how each stage works:

Stage 1 — Data ingestion Raw transactional data (payment type, amount, account balances, timestamps) is collected and stored as an initial dataset. This is the unprocessed source — it may contain missing values, noise, irrelevant columns, or imbalanced class distributions.

Pre-processing of data The raw data is cleaned and transformed into a final, model-ready dataset. Key steps include encoding categorical columns (like transaction type) using one-hot encoding, dropping non-predictive columns (like account name identifiers), and balancing the class distribution so the model sees roughly equal numbers of fraudulent and legitimate transactions.

Stage 2 — Data split The final dataset is divided into two non-overlapping subsets using a train-test split (typically 80/20 or 70/30). This is the critical step that prevents data leakage — the model learns only from the training set and is evaluated on the test set, which it has never seen.

Stage 3 — Model training The training data is fed into an ensemble of five algorithms: Logistic Regression (a probabilistic linear classifier), Random Forest Classifier (an ensemble of decision trees), Gaussian Naive Bayes (a probabilistic model based on Bayes' theorem), Decision Tree (a rule-based tree structure), and an Artificial Neural Network (a multi-layer perceptron that learns non-linear patterns). Using multiple models allows the system to compare performance and pick the best performer.

Stage 4 — Evaluation and output The test dataset is passed through each trained model. Performance is measured using metrics like accuracy, precision, recall, and ROC-AUC score. The final result is a binary classification — each transaction is labelled either as a **fraudulent transaction** (flagged for review or blocking) or a **non-fraudulent transaction** (approved for processing)

VII. Design & Implementation

Tools used

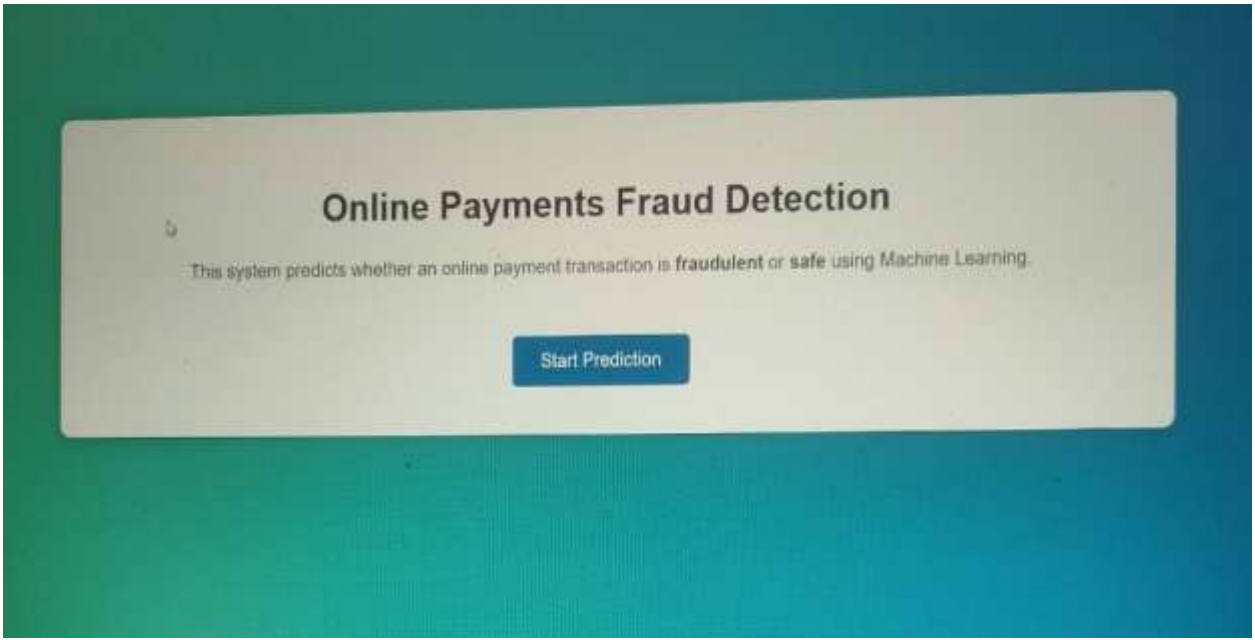
- Programming language: python
- IDE: VS code
- Libraries: Numpy, Pandas, Scikit-learn, Matplotlib, Flask

Steps

- Import dataset
- Data preprocessing
- Train machine learning model
- Test the model
- Build prediction interface

Display fraud detection resultThe trained model is integrated with a Flask web application. Users can upload an image, and the system processes the image and returns the predicted blood cell type.

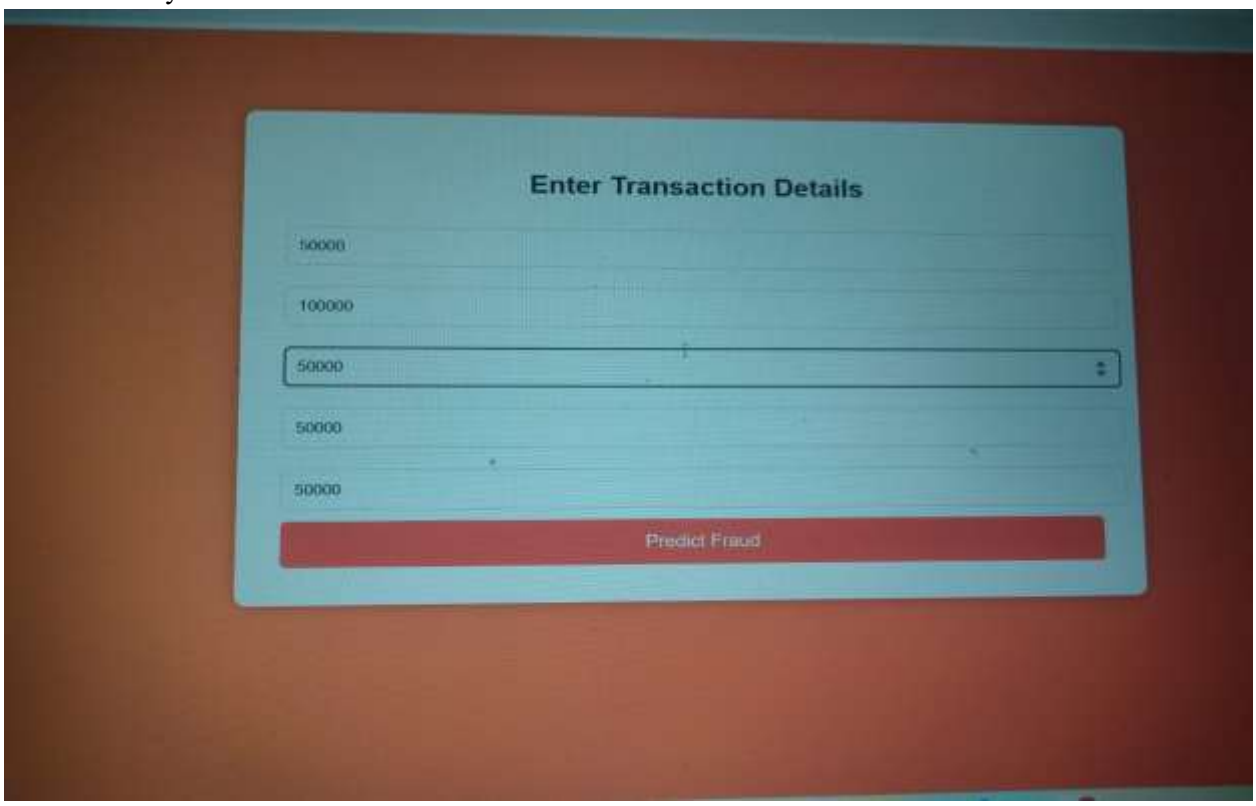
- Let's see what our output page looks like:



This image shows the **output/landing page** of the Online Payments Fraud Detection system. Here are 5 lines about it:

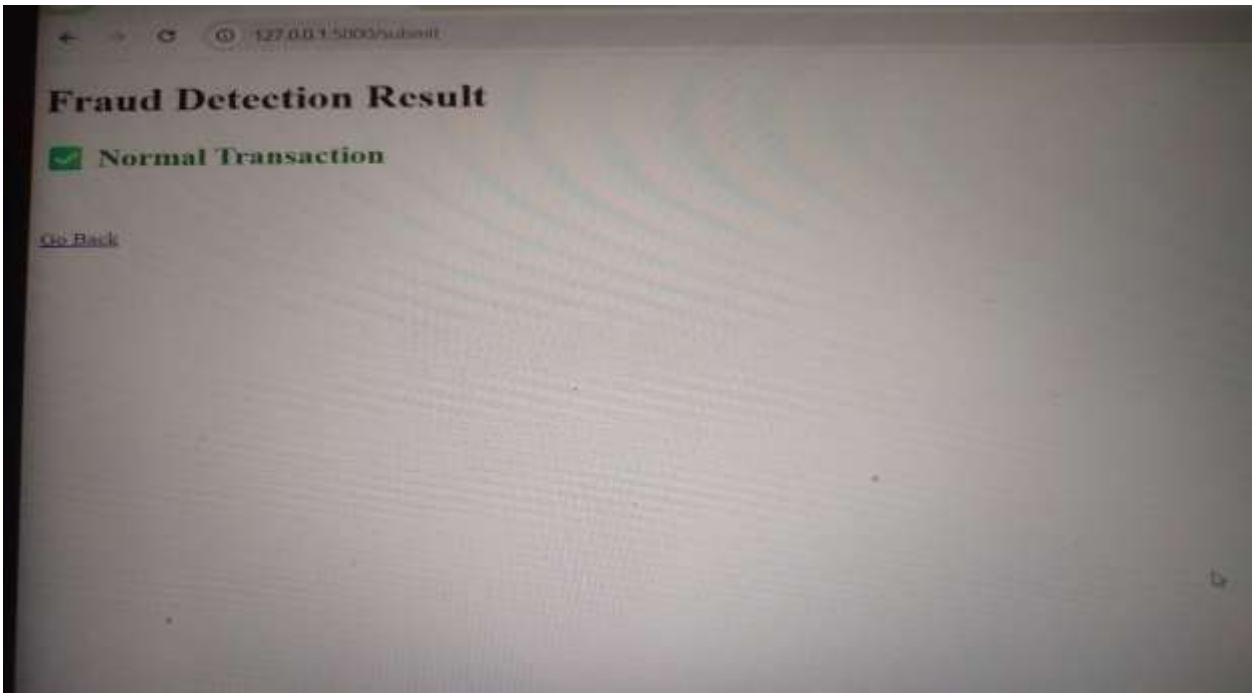
1. The page serves as the **entry point** of the fraud detection application, presenting a clean and minimal user interface with a title, brief description, and a call-to-action button.
2. The heading **"Online Payments Fraud Detection"** clearly communicates the purpose of the system — to identify whether a given online payment transaction is legitimate or fraudulent.
3. The descriptive text explains that the system uses **Machine Learning** to predict whether a transaction is **fraudulent** or **safe**, with both keywords visually highlighted in bold to draw user attention.
4. The **"Start Prediction"** button acts as the gateway to the input form, where users can enter transaction details such as type, amount, and account balances for the model to analyse.

5. The interface is built with a **simple, user-friendly design** — a white card on a teal gradient background — making it accessible and intuitive for non-technical users to interact with the ML-powered backend system.



This image shows the **"Enter Transaction Details"** input page of the fraud detection system.

1. The page presents a **structured input form** where users can manually enter the key financial attributes of a transaction — including the transaction amount, old balance, new balance of origin and destination accounts — which serve as feature inputs to the trained ML model.
2. The form contains **five input fields**, with sample values pre-filled (50000, 100000, 50000, 50000, 50000), representing transaction parameters such as amount, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest that directly correspond to the dataset features used during model training.
3. The **third field appears as a dropdown (spinner)** rather than a plain text box, likely representing the transaction type (e.g., PAYMENT, TRANSFER, CASH_OUT), which is a categorical variable encoded during preprocessing before being passed to the classifier.
4. The prominent **"Predict Fraud"** button in red at the bottom triggers the backend ML model to process the entered values, run them through the trained classifier (such as XGBClassifier or Random Forest), and return a prediction of whether the transaction is fraudulent or safe.
5. The page is styled with a **light card on an orange/red background**, clearly contrasting the landing page's teal theme, and the use of red for the action button reinforces the high-stakes, alert-oriented nature of fraud prediction — guiding the user's attention directly to the submit action.



This image shows the **"Fraud Detection Result"** output page of the system.

1. The page is served at the URL **127.0.0.1:5000/submit**, confirming that the application is built using **Flask** — a lightweight Python web framework — running on a local development server at port 5000, where the /submit route handles the POST request from the input form and returns the prediction result.
2. The heading **"Fraud Detection Result"** clearly indicates this is the final output page, displayed immediately after the ML model processes the submitted transaction details and generates a binary classification prediction.
3. The result is displayed as **"Normal Transaction"** accompanied by a **green checkbox icon**, which visually communicates that the entered transaction details were classified as **non-fraudulent (isFraud = 0)** by the trained machine learning model — providing an instant, easy-to-understand verdict.
4. The use of **green color and a tick mark** follows standard UI/UX conventions for safe or approved status, making the result immediately recognisable even to non-technical users — while a fraudulent transaction would likely be displayed in red with an alert icon for contrast.
5. The **"Go Back"** hyperlink at the bottom allows the user to return to the input form and test another transaction, enabling **repeated predictions** without restarting the application — demonstrating the system's practical usability as an interactive fraud detection tool.

VIII.Applications

- **Banking and Credit Card Fraud Prevention** — Detects unauthorized credit/debit card transactions in real time.
- **E-Commerce Payment Security** — Screens online checkout transactions to prevent stolen card usage.
- **UPI and Mobile Wallet Protection** — Monitors digital payment platforms like PhonePe and Google Pay for suspicious transfers.
- **Insurance Claim Fraud Detection** — Identifies false or exaggerated insurance claim submissions.
- **Online Travel Agency Fraud Prevention** — Filters fraudulent flight and hotel bookings made using stolen credentials.

IX.Conclusion

This study demonstrates the potential of machine learning in detecting online payment fraud. By analysing transaction data and developing robust models, we can significantly reduce the risk of fraud in online payments. Future work will focus on improving model accuracy and integrating the models into real-world systems. The ultimate goal is to create a secure and reliable online payment environment that protects both consumers and financial institutions from fraudulent activities.

n conclusion, the outlined methodology provides a structured approach for building and deploying a machine learning model for online fraud detection. By following these steps, organizations can effectively leverage data-driven techniques to mitigate the risks associated with fraudulent online transactions. Through the collection and preprocessing of relevant data coupled with the application of suitable machine learning algorithms, organizations can develop models capable of distinguishing between normal and fraudulent patterns. Rigorous training, testing, and validation processes ensure the accuracy and reliability of the model before deployment into real-world environments. Once deployed, the model becomes an integral component of the online fraud detection system, continuously analyzing transactions in real time to identify suspicious activities. Its effectiveness hinges on ongoing monitoring and periodic updates to adapt to evolving fraud tactics and maintain optimal performance. Ultimately, the adoption of machine learning for fraud detection not only enhances security but also contributes to the overall trust and integrity of online transactions, safeguarding both businesses and consumers against financial losses and reputational damage.

X.References

1. [N. Nanda, S. Choudhary, “Credit Card Fraud Detection Using Machine Learning,” *International Journal of Computer Applications*, 2018.
2. A. Kulkarni, “Fraud Detection in Credit Card Transactions Using Random Forest and LOF,” *IEEE Conference*, 2019.
3. T. Lalev, “Application of Deep Neural Networks in Fraud Detection,” *Journal of AI Research*, 2019.
4. M. Halsteinslid, “Detecting Fraud Using Logistic Regression,” *Norwegian University Research*, 2019.
5. J. Chen et al., “Deep Forest Model for Fraud Detection,” *IEEE Transactions on Neural Networks*, 2024.
6. S. Lv et al., “Hybrid Logistic-SVM Model for Fraud Detection,” *Expert Systems with Applications*, 2022.
7. G. Thimonier et al., “Anomaly Detection Techniques for Financial Fraud,” *Pattern Recognition Letters*, 2023.
8. Y. Ni et al., “Handling Imbalanced Data in Fraud Detection Using Boosting Techniques,” *IEEE Access*, 2024.
9. P. Papasavva et al., “AI-Based Payment Fraud Detection Systems,” *ACM Computing Surveys*, 2024.
10. M. Rahman et al., “Real-Time Fraud Detection in Online Transactions,” *International Journal of Information Security*, 2017.
11. D. Fernandes, “Security Analysis of Online Payment Systems,” *Journal of Cybersecurity*, 2013.
12. X. Yuan et al., “Deep Learning for Financial Fraud Detection,” *IEEE Conference on Big Data*, 2017.
13. R. Sharma et al., “Automation of Fraud Detection Using AI,” *International Journal of Advanced Computer Science*, 2023.
14. L. Yue et al., “GAN-Based Fraud Detection in Financial Systems,” *IEEE Transactions on AI*, 2025.
15. PCI Security Standards Council, “PCI DSS Requirements for Payment Security,” 2017.