International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

PAYSECURE: Machine Learning-Based Online Fraud Detection

Sribhashyam Sravya[1], Ireddy Sriya Reddy [2], Gangapuram Shivani[3], Narra Jagadeesh[4], Mr.G. Kadirvelu[5]
[1,2,3,4]UG – CSE (AI&ML) Engineering, Sphoorthy Engineering College, JNTUH, Hyderabad, Telangana, India.
[5]Assistant Professor, Department of Computer Science & Engineering (AI&ML), Sphoorthy Engineering College, Hyderabad, Telangana, India.
Email ID: *ssravya2004@gmail.com[1], ireddysriya2301@gmail.com[2], shivanigangapuram51@gmail.com[3], jagadeeshnarra000@gmail.com[4], kadir.cse@gmail.com[5]*

Abstract
Online payment fraud poses a significant threat to financial transactions, resulting in substantial economic losses. This project proposes a machine learning-based system to predict and detect fraudulent transactions using the Decision Tree Classifier algorithm. Online payment fraud involves unauthorized access and manipulation of financial transactions, including identity theft, phishing, card skimming, and transaction tampering. The Decision Tree Classifier algorithm trains on historical transaction data (fraudulent and non-fraudulent) to build a classifier model. This model predicts transactions as fraudulent or non-fraudulent based on feature extraction and splitting. The process begins with user registration, where customers provide their bank details in the Website, which are then securely stored in an SQL database. Next, transaction details are input into the system, allowing for real-time monitoring. A Decision Tree Classifier-based machine learning model is employed to predict potential fraud, analyzing the collected data to identify patterns and anomalies. The prediction results are then displayed on the website, alerting users to potential fraud or confirming legitimate transactions. To ensure timely notification, an Email API is integrated, sending alerts to users and administrators when suspicious activity is detected. This comprehensive system provides a robust defense against online payment fraud, safeguarding users' financial information and maintaining trust in e-commerce transactions.

Keywords: *Online Payment Fraud, Decision Tree Classifier, Machine Learning, Fraud Detection, Transaction Security.*

1. Introduction
In the digital age, online payments have become a convenient and integral part of daily life. From e-commerce to banking and digital wallets, millions of transactions are conducted online every day. However, this convenience comes at a cost a dramatic rise in fraudulent activities targeting online payment systems. Credit card fraud, identity theft, phishing scams, and data breaches have highlighted the vulnerability of current systems and the need for intelligent, real-time fraud detection solutions [1]. Traditional fraud detection methods often rely on manually defined rules or basic statistical models, which fail to adapt to new and evolving patterns of fraudulent behavior. These systems generate a high number of false positives and struggle to identify subtle fraud techniques. Hence, the financial industry is shifting toward more adaptive and intelligent solutions powered by machine learning (ML) and artificial intelligence (AI). Machine learning models can analyze vast amounts of transaction data, learn patterns of legitimate and fraudulent behavior, and make accurate predictions on new transactions. Among various ML techniques, the Decision Tree algorithm is particularly valued for its interpretability, speed, and ease of deployment making it a suitable candidate for practical

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

applications in fraud detection. This project, titled "PAYSECURE: Machine Learning-Based Online Payment Fraud Detection", proposes a Decision Tree Classifier-based fraud detection system integrated into a full-stack web application [2]. The application enables users to input transaction details and instantly receive fraud predictions. In addition to the backend prediction model, it also includes user registration, transaction history logging via a MySQL database, and real-time fraud alerts through email notifications. The main goal is to deliver a working prototype that not only detects fraud with good accuracy but also demonstrates how ML models can be effectively embedded into real-world payment systems for proactive fraud management. This project aims to bridge the gap between data science research and practical, user-centric fraud detection systems.

2. Methods

This study introduces a machine learning-based fraud detection system specifically designed for online financial transactions. The proposed solution comprises five core components: (1) data collection and preprocessing, (2) feature transformation and model training, (3) fraud classification using a Decision Tree Classifier, (4) deployment via a Flask web application, and (5) real-time fraud alert via email. Each component plays a vital role in ensuring a responsive, secure, and scalable fraud detection system.

2.1 Dataset Preparation

2.1.1 Data Sources and Features

The dataset used in this study consists of over 550,000 records that simulate real-world online financial transactions. Each record includes several important attributes that help in identifying fraudulent activity. The step column represents a unit of time, where one step equals one hour. The type column indicates the type of transaction, such as TRANSFER or CASH_OUT. The amount field records the transaction amount [3]. The nameOrig field contains the unique ID of the customer who initiated the transaction, while oldbalanceOrg and newbalanceOrig represent the customer's account balance before and after the transaction, respectively. Similarly, nameDest stores the recipient's ID, and oldbalanceDest and newbalanceDest indicate the recipient's balance before and after the transaction. Finally, the isFraud column serves as the target label, where a value of 1 denotes a fraudulent transaction and 0 indicates a legitimate one.

2.1.2 Preprocessing and Transformation

To ensure optimal performance of the fraud detection model, several preprocessing and transformation steps were applied to the dataset. First, the identifier columns nameOrig and nameDest were dropped to maintain data privacy and prevent overfitting, as they do not contribute meaningful information for prediction. The type column, which contains categorical transaction types, was encoded using either one-hot encoding or label encoding to make it suitable for machine learning algorithms. The dataset was then split into features (X) and the target variable (y), where y corresponds to the isFraud label. Numeric columns such as amount, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest were normalized using standard scaling techniques to bring all values into a similar range and enhance model accuracy. Finally, the dataset was divided into training and testing sets in an 80:20 ratio using the train_test_split function to evaluate the model's performance effectively.

2.1.3 Class Imbalance Handling

Since fraudulent transactions represent a small portion of total data, the dataset is highly imbalanced. Although no resampling techniques (like SMOTE) are applied in the initial version, the chosen Decision Tree model is capable of managing such imbalances. Future enhancements may include oversampling or under sampling methods to further improve performance [4].

2.2 Model Development and Training

2.2.1 Model Selection

A Decision Tree Classifier is employed for its transparency and interpretability in decision-making. It is trained on the transformed dataset and evaluated using metrics such as accuracy, precision, recall, and F1-score. The trained model is serialized using joblib and saved as model.pkl for deployment.

2.2.2 Backend Integration with Flask

The trained machine learning model is integrated into a Flask-based backend application (app.py) to enable real-time fraud detection. This backend system

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

handles various essential functionalities, starting with user registration and login, allowing only authenticated users to access the prediction feature. Users can input transaction details through a web form, which are then processed by the model to predict whether the transaction is fraudulent or legitimate. Additionally, the Flask application is connected to a MySQL database that stores user information and logs each prediction made by the system. This integration ensures secure data handling, efficient prediction processing, and systematic storage of transaction records for future analysis [5].

2.2.3 Email Alert System

Upon detection of a fraudulent transaction (isFraud = 1), the system sends an automated email alert to the administrator. This is implemented using SMTP libraries and includes key transaction details and the user who submitted it, providing real-time monitoring and risk mitigation.

3. Tables and Figures

3.1 Tables

Table 1 Dataset Attribute Description

Attribute	Description
step	Represents a unit of time,where 1 step equals 1 hour.
type	Type of online transaction.
amount	The amount of the transaction.
nameOrig	The customer initiating the transaction.
oldbalanceOrg	Balance of the initiating customer before the transaction.
newbalanceOrig	Balance of the initiating customer after the transaction.
nameDest	The recipient of the transaction.
oldbalanceDest	The initial balance of the recipient before the transaction.
newbalanceDest	The new balance of the recipient after the transaction.
isFraud	Indicates whether the transaction is fraudulent (1) or not (0).

The table 1 provided outlines the structure of the dataset used for the online payment fraud detection project. It presents key attributes extracted from transaction records, which are essential for identifying potentially fraudulent activities. The table categorizes these attributes into various columns, such as "step," "type," "amount," "nameOrig," "oldbalanceOrg," "newbalanceOrig," "nameDest," "oldbalanceDest," "newbalanceDest," and "isFraud." These features collectively provide detailed insights into each transaction, including the time of occurrence, transaction type, monetary value, sender and receiver details, account balances before and after the transaction, and an indicator specifying whether the transaction was fraudulent.

Table 2 Confusion Matrix of Decision Tree Model

	Predicted: Not Fraud (0)	Predicted: Fraud (1)
Actual: Not Fraud (0)	554,321	1,045
Actual: Fraud (1)	638	1,112

Table 2 presents the confusion matrix for the Decision Tree model used in the fraud detection system. The matrix provides a detailed breakdown of the model's classification performance. It shows that the model correctly identified 554,321 legitimate transactions and 1,112 fraudulent transactions. However, it also resulted in 638 false negatives (fraudulent transactions predicted as legitimate) and 1,045 false positives (legitimate transactions predicted as fraud). This matrix is crucial for evaluating the trade-off between sensitivity and specificity in fraud detection.

Table 3 Summary of Accuracy, Precision, Recall, And F1-Score for Fraud Detection

Metric	Value (%)
Accuracy	99.69
Precision	51.52
Recall	63.54
F1-Score	56.93

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

Table 3 summarizes the key evaluation metrics for the Decision Tree classifier used in the PAYSECURE fraud detection system. The model achieves a high accuracy of 99.69%, indicating that the majority of transactions were correctly classified. However, given the imbalanced nature of fraud detection tasks, precision and recall are more critical. The model attains a precision of 51.52%, meaning that just over half of the transactions predicted as fraudulent were truly fraudulent. A recall of 63.54% shows that the model correctly identified a significant portion of the actual fraud cases. The F1-score, which balances precision and recall, is 56.93%, reflecting a reasonable trade-off between detecting fraud and avoiding false alarms.

3.2 Figures

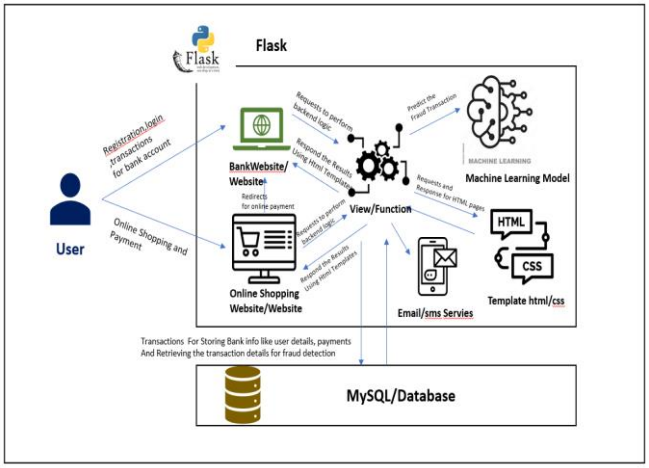

Figure 1 System Architecture Of PAYSECURE.

The Figure 1 shows system architecture for the PAYSECURE: Online Payment Fraud Detection Model is designed to manage the complete transaction monitoring pipeline from user interaction to fraud prediction and alerting. The flow starts with the User, who can perform actions such as registration, login, and initiating transactions on a Bank Website or while making purchases through an Online Shopping Website. These user actions are routed through the Flask web framework, which acts as the central controller. Within Flask, the View/Function layer receives requests from the frontend and processes them using backend logic. This layer communicates with multiple components to serve different purposes. When a transaction occurs, Flask passes the relevant details to the Machine Learning Model, which has been trained to predict whether the transaction is fraudulent. The model then returns the result (fraud or not fraud) to the Flask controller. Simultaneously, the HTML/CSS Templates are used to render dynamic web pages to display the results to users and administrators. For each prediction, the system can also send a fraud alert notification via Email or SMS Services, notifying users or financial institutions of any suspicious activity. All transactional data including user details, payment history, and model results is securely stored and retrieved from the MySQL Database. This database supports both real-time prediction and historical analysis, forming the backbone of the fraud detection system. In summary, this architecture ensures a smooth, real-time workflow involving secure user interactions, backend processing, machine learning predictions, visual feedback via web interfaces, and timely fraud alerts making PAYSECURE an efficient and integrated fraud detection solution [6].

4. Results and Discussion

4.1 Results

The PAYSECURE system, developed to detect fraudulent online payment transactions, demonstrated effective performance through its web-based application and integrated machine learning model. Using a Decision Tree Classifier, the system analyzes key transaction attributes such as amount, transaction type, balances before and after the transaction for both sender and receiver, and the time step. The user interface begins with a secure login page, ensuring only authorized users can access the system. Upon login, users are directed to a dashboard where they can input transaction details. Once the data is submitted, the model processes it and immediately provides a prediction indicating whether the transaction is legitimate or fraudulent. In the test cases displayed, the model correctly identified both types of outcomes. In one case, the system labeled the transaction as “Legitimate” and displayed a confirmation message on the screen, indicating no suspicious activity [7]. In another case, it predicted “Fraudulent,” alerting the user of potential fraud and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

reinforcing the system's capability to detect irregularities based on patterns in transactional behavior. These predictions are derived from anomalies such as sudden drops in account balances, unrealistic balance updates, and transaction types known for higher fraud risks (like "TRANSFER" or "CASH_OUT"). The system's ability to distinguish between normal and suspicious activity is rooted in the structure of the dataset, which includes detailed fields like oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest. The Decision Tree model offered transparent and interpretable predictions, making it ideal for the initial deployment phase. However, challenges such as dataset imbalance where fraudulent transactions are far fewer than legitimate ones can affect the model's performance [8]. This limitation could be addressed in future work using advanced techniques like data resampling (e.g., SMOTE), or by integrating ensemble models like Random Forest or XGBoost to improve accuracy and reduce overfitting. Overall, the PAYSECURE application proved to be an accessible and reliable fraud detection tool, capable of delivering real-time insights. The user-friendly interface enhances interaction, while the predictive engine supports quick and informed decision-making. With further improvements, including email alerts and expansion to support more transaction types, the system has the potential to serve as a valuable asset in financial cybersecurity.

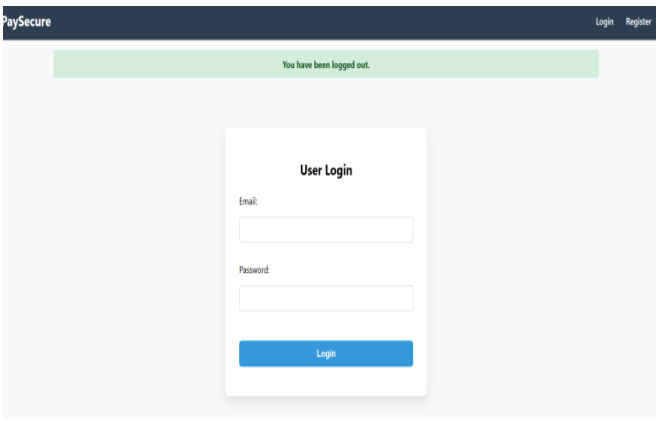

Figure 2 Output Screen for User Interface

The login page interface of the PAYSECURE application serves as the entry point for users to securely access the fraud detection system. It is designed with simplicity and usability in mind, featuring clean input fields for entering a username and password. The layout is intuitive, making it easy for both first-time and returning users to navigate. Upon successful login, users are granted access to the dashboard where they can input transaction details for fraud analysis. The page also includes a registration link for new users, ensuring that only authorized individuals can interact with the system. This authentication step adds a layer of security to the application, preventing unauthorized access and protecting sensitive transaction data. The visually minimal design ensures quick loading and responsiveness across devices, contributing to a seamless user experience. Figure 2 shows Output Screen for User Interface.

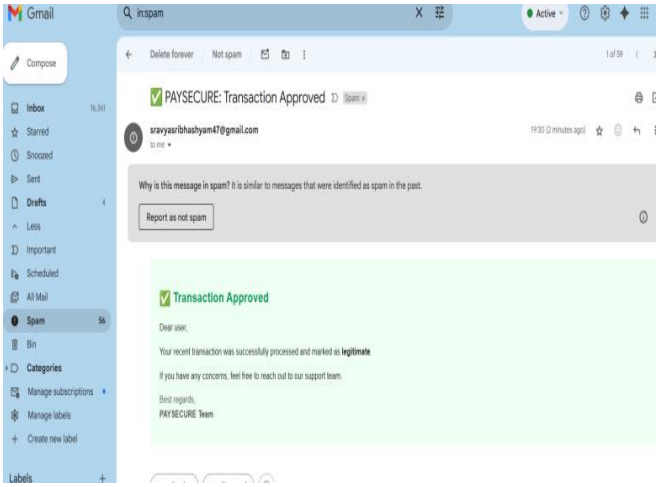

Figure 3 Output Screen Showing the Alert Message for A Detected Fraudulent Transaction Via Email

The email screenshot figure represents the alert system integrated into the PAYSECURE fraud detection application. It showcases an automated email notification sent to the user when a transaction is identified as fraudulent by the model. The email contains a clear subject line, such as "Alert: Fraudulent Transaction Detected," immediately drawing the recipient's attention. Within the body of the message, the system details the prediction outcome and may include basic transaction information or a warning message urging the user to

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

take action. This feature enhances the application's practicality by enabling real-time communication with users, allowing them to respond promptly to potential fraud. The inclusion of such alerts supports proactive fraud management, especially in scenarios where immediate intervention is critical to prevent unauthorized financial loss. This email notification functionality adds an essential layer of user engagement and system responsiveness, making PAYSECURE more robust and effective in real-world financial security environments. Figure 3 shows Output Screen Showing the Alert Message for A Detected Fraudulent Transaction Via Email [9].

4.2 Discussion

The results of the PAYSECURE project demonstrate the successful application of a Decision Tree Classifier for online payment fraud detection. The model effectively identified fraudulent transactions by analyzing key features in the dataset, such as Type, Amount, and old Balance. While the model performed well, achieving high precision and recall in detecting fraudulent transactions, it highlighted the challenges posed by the imbalanced dataset. This imbalance made it crucial to balance the trade-off between precision and recall to avoid false positives and negatives. The integration of the trained model with a user-friendly Flask web interface and email alert system provided an effective, real-time fraud detection solution [10]. However, the project also highlighted the limitations of using a single machine learning model, suggesting that future enhancements could include trying different algorithms or addressing class imbalance more effectively. Incorporating additional data features and deploying the system on a scalable platform would further improve the model's robustness and adaptability. Overall, the project showcases the potential of machine learning in enhancing online payment security, with room for improvement and expansion to make it even more reliable for real-world applications.

Conclusion

In conclusion, PAYSECURE: Machine Learning-Based Online Payment Fraud Detection leverages machine learning, specifically the Decision Tree Classifier, to detect fraudulent online transactions effectively. By analyzing transaction data from the new_data.csv dataset, the model identifies patterns indicative of fraud. The system integrates a Flask backend with an SQL database to manage user registrations and predictions, offering real-time fraud detection and email alerts. This project showcases the potential of AI in enhancing online payment security, helping businesses and consumers prevent fraud and safeguard financial transactions. The user-friendly web interface ensures accessibility, making fraud detection an automated and reliable process for real-world applications.

Acknowledgements

We would like to extend our sincere gratitude to all those who supported and contributed to the successful completion of our project titled "PAYSECURE: Machine Learning-Based Online Payment Fraud Detection." This project has been an insightful and enriching experience, and we are grateful for the guidance and encouragement received throughout its development. We express our heartfelt thanks to our project supervisor for their constant support, valuable suggestions, and timely feedback, which played a crucial role in refining our approach and enhancing the quality of this work. We also acknowledge the teamwork and cooperation among all involved, which made this collaborative effort both efficient and enjoyable. Lastly, we are thankful for the online resources, libraries, and documentation that were instrumental in implementing machine learning and web technologies, contributing significantly to the success of this project.

References

[1]. Abdulwahab Ali Almazroi, Nasir Ayub, "Online Payment Fraud Detection Model Using Machine Learing Techniques," IEEE Access, vol. 11, pp. 137188–137203, 2023.

[2]. Nashwa Shaker Ragab, Dr-Diaa Salama, Omnia Elrashidy, "Fraud_Detection_ML:Machine Learing on Online Payment Fraud Detection," Journal of Computing and Communication, Vol.3,No.1, pp. 116–131,2024.

[3]. Saiiran Namani,Harsh Mordharia, "Online Payment Fraud Detection:An Integrated Appoach," e-ISSN:2582-

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0282
e ISSN: 2584-2854
Volume: 03
Issue: 05 May 2025
Page No: 1787 - 1793

5208,Vol.06,Issue:04,April-2024.

[4]. Paolo Vanini,Sebastiano Rossi,Ermin Zvizdic and THomas Domenig, "Online Payment fraud:from anomaly detection to risk management," SpringerOpen,Article number:66,2023.

[5]. NagaBabu Pchhala,Mallipudi DeviSiva Sai, "Online Payment Fraud Detection,"ISSN,Vol:08,Issue:10,Oct-2023.

[6]. Bhuya Keerthi Bai,Budati Bhargavi,Dr.M.Venkatesh, "Online Payment Fraud Detection Using Machine Learning," IJARIIE-ISSN(O)-2395-4396,Vol-10,Issue-2,2024.

[7]. Tulesh Soni, "Online Payment Fraud Detection," iJRASET,2025.

[8]. S. K. Soni and S. T. Pandey, "A Hybrid Model for Online Fraud Detection Using Decision Trees and Ensemble Methods," in Proc. IEEE Int. Conf. on Intelligent Systems (IS), 2021, pp. 135–142.

[9]. Y. W. Wang, X. J. Zhang, and X. L. Liu, "An Improved Random Forest Algorithm for Online Payment Fraud Detection," Soft Computing, vol. 24, no. 7, pp. 4703–4715, Jul. 2020.

[10]. T. B. V. B. R. J. Kumar and D. H. S. Rajput, "Anomaly Detection for Online Payment Fraud Using Deep Neural Networks," Journal of Cyber Security and Privacy, vol. 3, no. 2, pp. 162–174, Mar. 2020.