IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

Online Payment Fraud Detection Using Machine Learning Techniques

Prof. Rahul P. Bembade[1], Kunal V. Masurkar[2], Rushikesh P. Gaikawad[3], Adhiraj S. Nimbalkar[4], Dhruv P. Parmar[5]

Assistant Professor, Computer Science & Engineering [1]
Students, Computer Science & Engineering[2,3,4,5]
MIT Arts, Commerce and Science Co**ll**ege, Loni **K**a**lbh**or, Pune, India

Abstract: *Online payment systems have revolutionized global commerce, but they have also increased exposure to fraudulent activities. This research paper presents a comprehensive approach to identifying fraudulent transactions using machine learning techniques. The proposed models are evaluated on a publicly available dataset from Kaggle, where historical transactional data is used for training and testing. Among the models tested, the Random Forest classifier achieved the best performance, with an F1-score of 0.95. This paper also addresses the challenge of class imbalance and highlights the importance of precision in minimizing false positives in fraud detection systems.*

Keywords: Online Payments, Fraud Detection, Machine Learning, Random Forest, Class Imbalance

I. INTRODUCTION

With the increasing adoption of online payments, safeguarding financial transactions has become crucial. According to a recent report, online payment fraud losses reached billions of dollars globally, necessitating the development of advanced fraud detection systems. Traditional rule-based approaches have shown limitations in adapting to evolving fraud patterns. Therefore, machine learning models capable of identifying complex data patterns have emerged as a promising solution.

This study aims to apply and compare various machine learning algorithms to detect fraudulent transactions using a dataset from Kaggle. Our primary objective is to find the most effective model for accurate fraud detection while minimizing false positives.

II. METHODOLOGY

The research methodology comprises the following steps:

Dataset Description

The dataset used in this study contains a total of 284,807 transactions, of which only 0.17% are labelled as fraudulent. Each transaction is represented by 30 features, including transaction time, amount, and anonymized attributes.

- Dataset Source: Kaggle (Credit Card Fraud Detection)
- Number of Features: 30
- Class Distribution: Imbalanced, with only 492 fraudulent transactions.

Data Preprocessing

- Feature Scaling: Standard Scaler was applied to normalize continuous features like Amount and Time.
- Class Balancing: Since the dataset is highly imbalanced, techniques like SMOTE (Synthetic Minority Over-sampling Technique) were used to generate synthetic samples for the minority class.
- Train-Test Split: The data was divided into training (80%) and testing (20%) sets to evaluate model performance.

Model Implementation

Three primary machine learning models were implemented and tested:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

- Decision Tree: A simple baseline model for initial testing.
- Random Forest: An ensemble method that combines multiple decision trees to improve accuracy.
- Neural Networks: Constructed using Keras with two hidden layers and ReLU activation.

Evaluation Metrics

- Accuracy: The proportion of correctly classified transactions.
- Precision: Measures the accuracy of positive predictions.
- Recall: Measures how many actual fraudulent transactions are correctly identified.
- F1-Score: Balances precision and recall for an overall performance measure.

III. IMPLEMENTATION AND RESULTS

The models were evaluated on the hold-out test set to measure their effectiveness in detecting fraudulent transactions. Each model was trained using various hyperparameters, and extensive cross-validation was performed to ensure the results were not due to random chance. The key results for each model are summarized below:

Decision Tree

The Decision Tree model was used as a baseline to establish the fundamental structure of the data and to identify key features that differentiate fraudulent transactions from legitimate ones. Although the Decision Tree achieved an accuracy of 89%, it exhibited a tendency to overfit on the training data. This was evident from its significantly lower precision and recall scores on the test set, making it unsuitable for a highly imbalanced dataset like this. The model struggled with generalization due to its nature of creating overly specific rules for each class.

- Accuracy: 89%
- Precision: 0.81
- Recall: 0.73
- F1-Score: 0.77

Random Forest

The Random Forest model, an ensemble of multiple decision trees, performed significantly better. By aggregating the results of multiple trees, the model reduced overfitting and captured complex patterns in the data. It achieved the highest overall performance with an F1-score of 0.95 and an ROC-AUC score of 0.98. The high ROC-AUC indicates that the model was able to differentiate between fraudulent and non-fraudulent transactions effectively.

Additionally, implementing SMOTE (Synthetic Minority Over-sampling Technique) for balancing the dataset improved the recall score by 15%, ensuring more fraudulent transactions were correctly identified. This is crucial in fraud detection, where missing even a single fraudulent transaction could result in significant financial loss.

- Accuracy: 97%
- Precision: 0.94
- Recall: 0.96
- F1-Score: 0.95
- ROC-AUC: 0.98

Neural Networks

The Neural Network model was constructed using a multi-layer perceptron (MLP) with two hidden layers and the ReLU activation function. While the network captured intricate relationships between features, it required extensive hyperparameter tuning to handle the imbalanced dataset effectively. The network showed good potential but was slightly less effective than Random Forest due to its sensitivity to noise in the data.

To address the class imbalance, various techniques such as class weighting and oversampling were applied. However, these modifications increased the training complexity and time. Despite these efforts, the Neural Network achieved a decent F1-score but still fell short of Random Forest's performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

- Accuracy: 94%
- Precision: 0.90
- Recall: 0.91
- F1-Score: 0.90
- ROC-AUC: 0.95

Comparison and Analysis

The comparative analysis revealed that the Random Forest model was the best performer in terms of overall accuracy, precision, recall, and F1-score. The ensemble method's ability to aggregate multiple trees allowed it to identify subtle patterns indicative of fraud, such as small transaction amounts occurring at unusual times or transactions originating from uncommon locations. These patterns were often missed by other models.

Furthermore, the application of SMOTE effectively reduced the issue of class imbalance, resulting in a better recall score (96%) compared to other models. However, the increase in recall came at a slight cost of a few more false positives, which could be manageable in a real-world scenario, where identifying fraudulent transactions is the primary objective.

Visual Analysis of Model Performance

To better understand the model's performance, confusion matrices and ROC curves were plotted for each model:

- **Confusion Matrix**: Showed the distribution of true positives, false positives, true negatives, and false negatives. The Random Forest model showed a high number of true positives, indicating its effectiveness.
- **ROC Curve**: Plotted for each model to visualize the trade-off between the true positive rate and false positive rate. The Random Forest model had the highest area under the curve, signifying its strong performance.

These visual insights helped pinpoint areas of improvement and guided future enhancements for handling edge cases.

IV. CONCLUSION

This paper demonstrated the potential of machine learning models in detecting fraudulent online payments. By leveraging historical transaction data and employing advanced preprocessing techniques such as SMOTE, the models were able to distinguish fraudulent activities with high precision and recall. The Random Forest model outperformed other models, achieving the highest accuracy and F1-score, making it a strong candidate for real-world applications.

However, several challenges need to be addressed to make these models more robust and reliable. The primary issue lies in handling the extreme class imbalance, which can lead to biased predictions. Additionally, fraud patterns continuously evolve as fraudsters adapt to detection strategies, making it crucial to implement real-time monitoring systems that can dynamically learn from new data. Future work could focus on integrating additional contextual features, such as user behavior and network-based features, to improve detection capabilities further.

Moreover, considering the computational cost of deploying complex models like Neural Networks, optimization techniques could be explored to balance detection accuracy and system efficiency. By incorporating these improvements, the proposed models can be adapted to a wide range of online payment systems, reducing financial losses and ensuring a safer transaction environment.

REFERENCES

[1]. Breiman, L. (2001). "Random Forests." Machine Learning, 45(1), 5-32.

[2]. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). "SMOTE: Synthetic Minority Over-sampling Technique." Journal of Artificial Intelligence Research, 16, 321-357.

[3]. Chen, T., & Guestrin, C. (2016). "XGBoost: A Scalable Tree Boosting System." Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.

[4]. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). "A Comprehensive Survey of Data Mining-based Fraud Detection Research." arXiv preprint arXiv:1009.6119.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

[5]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). "Data Mining for Credit Card Fraud: A Comparative Study." Decision Support Systems, 50(3), 602-613.

[6]. Sahin, Y., & Duman, E. (2011). "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines." Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol. 1, IMECS 2011.

[7]. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). "Fraud Detection System: A Survey." Journal of Network and Computer Applications, 68, 90-113.

[8]. West, J., & Bhattacharya, M. (2016). "Intelligent Financial Fraud Detection: A Comprehensive Review." Computers & Security, 57, 47-66.