

Credit card fraud detection using Machine Learning

Mr. G . Suresh Kumar¹, N. Naga Swetha², V. Yuvaraj Yugesh², V. Jaya Sai Venkata Murari² V. Sanjay², P. N. Ashish².

¹ Assistant Professor, Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, 534202

² Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, 534202

Abstract

The project, titled "Credit Card Fraud Detection using Machine Learning - XGBoost," addresses the crucial need for credit card companies to identify fraudulent transactions and protect customers from unauthorized charges. The dataset comprises credit card transactions in September 2013, with 492 frauds out of 284,807 transactions, resulting in a highly imbalanced class distribution (0.172% frauds). Due to confidentiality, only numerical features resulting from Principal Component Analysis (PCA) are provided, with 'Time' and 'Amount' being the only non-PCA transformed variables. The proposed solution leverages the XGBoost algorithm, a powerful machine learning technique, to effectively distinguish between legitimate and fraudulent transactions. The 'Time' feature captures the elapsed seconds from the first transaction, while 'Amount' represents the transaction amount, facilitating dynamic cost-sensitive learning. Given the class imbalance, the evaluation metric recommended is the Area Under the Precision-Recall Curve (AUPRC), ensuring a more meaningful assessment than traditional confusion matrix accuracy. This project aims to contribute to the enhancement of fraud detection systems in the financial sector, emphasizing the importance of precision and recall in evaluating model performance within the context of imbalanced datasets.

Keywords: Fraud detection, Applications of Machine Learning, XGBoost, Decision Tree, Random Forest

1. Introduction

The prevalence of fraudulent credit card transactions poses a significant challenge for both credit card companies and cardholders. In the era of digital transactions, it has become crucial to develop robust systems capable of detecting and preventing unauthorized activities. The dataset under consideration encompasses credit card transactions conducted by European cardholders in September 2013. Within this limited timeframe, the dataset reveals a stark reality – among 284,807 transactions, 492 are identified as fraudulent, accounting for a mere 0.172% of the total transactions. This striking class imbalance emphasizes the urgency of implementing effective fraud detection mechanisms.

The real-life problem at hand revolves around the financial losses and inconvenience suffered by customers when their credit cards are used for unauthorized transactions. Traditional methods of fraud detection may fall short in handling the intricacies of modern cyber threats. The project aims to leverage machine learning, specifically the XGBoost algorithm, to address this issue. By harnessing the power of predictive modeling, the goal is to develop a system capable of identifying fraudulent transactions with high precision.

Machine learning plays a pivotal role in this context by automating the detection process and continuously adapting to evolving fraud patterns. The dataset's numerical features, resulting from a Principal Component Analysis (PCA) transformation, provide an anonymized representation of transaction characteristics. The 'Time' feature denotes the elapsed seconds between transactions, and the 'Amount' feature signifies the transaction amount – crucial aspects for discerning anomalous behavior. The utilization of XGBoost, known for its efficiency and accuracy in handling imbalanced datasets, positions the project to effectively navigate the challenges posed by the skewed distribution of fraud instances.

The beneficiaries of this machine learning-based fraud detection system are multi-faceted. Firstly, credit card companies stand to gain by minimizing financial losses associated with fraudulent transactions. Enhanced fraud detection not only safeguards customers' funds but also helps maintain the integrity of financial systems. Cardholders, on the other hand, benefit from increased security and reduced inconvenience caused by unauthorized transactions. Furthermore, the project contributes to the broader landscape of cybersecurity, demonstrating the practical application of advanced analytics in mitigating financial risks. Ultimately, the successful implementation of the Credit Card Fraud Detection project using XGBoost not only safeguards financial transactions but also establishes a scalable and adaptive framework for addressing emerging challenges in the realm of cybersecurity.

The dataset consists of numerical features resulting from a Principal Component Analysis (PCA) transformation, with only 'Time' and 'Amount' remaining unaltered. The 'Time' feature represents the seconds elapsed since the first transaction, while 'Amount' denotes the transaction amount. The response variable, 'Class,' takes the value 1 in case of fraud and 0 otherwise.

Given the class imbalance, traditional accuracy metrics are inadequate, prompting the use of the Area Under the PrecisionRecall Curve (AUPRC) for evaluation. The project focuses on employing the XGBoost machine learning algorithm to build a robust model for fraud detection. Despite the confidentiality constraints preventing the disclosure of original features and additional background information, the project aims to showcase the efficacy of XGBoost in handling imbalanced datasets for enhanced credit card fraud detection.

2. Literature Survey

1. Chaudhary, Khyati, Jyoti Yadav, and Bhawna Mallick. "A review of fraud detection techniques: Credit card." *International Journal of Computer Applications* 45.1 (2012): 39-44. This paper addresses the growing concern of credit card fraud in today's digital era, emphasizing the need for effective fraud detection. With the rise in credit card transactions, fraud has become a million-dollar business, posing significant economic challenges globally. The paper explores various fraud types, including credit card fraud, telecommunication fraud, computer intrusion, bankruptcy fraud, theft fraud, and application fraud. It highlights the importance of employing modern techniques like data mining, machine learning, and artificial intelligence for detecting fraudulent transactions. The aim is to develop models that combine high fraud coverage with a low false alarm rate. The study emphasizes the critical role of secure credit services and reliable fraud detection systems to ensure the safe usage of credit cards in the evolving landscape of electronic commerce.
2. Dal Pozzolo, Andrea, et al. "Learned lessons in credit card fraud detection from a practitioner perspective." *Expert systems with applications* 41.10 (2014): 4915-4928. This paper addresses the challenge of credit card fraud detection, where billions of dollars are lost annually. The focus is on creating effective algorithms using machine learning to combat fraud, considering issues like imbalanced data, changing patterns, and limited public datasets due to confidentiality. The study utilizes a real credit card dataset from an industrial partner to compare various algorithms and address key questions. It explores the choice of machine learning algorithms, the frequency of model updates, the impact of imbalanced data, and optimal strategies for fraud detection. The paper emphasizes the importance of adapting to changing environments in realtime and provides insights for practitioners dealing with large credit card datasets.
3. Patidar, Raghavendra, and Lokesh Sharma. "Credit card fraud detection using neural network." *International Journal of Soft Computing and Engineering (IJSCE)* 1.32-38 (2011). This paper explores the use of artificial neural networks (ANNs) and genetic algorithms for detecting credit card fraud in online transactions. With the rapid growth of online services in the payment card industry, there is an increased vulnerability to fraudulent activities. The paper suggests training ANNs with supervised learning to mimic the human brain's pattern recognition abilities, using past transaction data. Genetic algorithms are employed to optimize the neural network's architecture for efficient fraud detection. The study classifies fraud into different types, including merchant-related and internet-related frauds, highlighting the need for advanced detection methods. The proposed approach aims to enhance efficiency in identifying fraudulent transactions, considering the evolving techniques used by fraudsters.
4. Dal Pozzolo, Andrea, et al. "Credit card fraud detection: a realistic modeling and a novel learning strategy." *IEEE transactions on neural networks and learning systems* 29.8 (2017): 3784-3797. This paper addresses credit card fraud detection challenges in real-world scenarios, considering issues like concept drift, class imbalance, and verification latency. The authors propose a realistic model of fraud detection systems (FDS) and introduce appropriate performance measures.

They present a novel learning strategy that effectively handles class imbalance, concept drift, and verification latency. Experiments with over 75 million credit card transactions demonstrate the impact of class imbalance and concept drift. The study emphasizes the importance of considering the practical aspects of FDS, such as the alert–feedback interaction and verification latency, which are often overlooked in existing literature. The proposed approach aims to improve the precision of fraud alerts, crucial for real-world fraud detection systems.

5. Varmedja, Dejan, et al. "Credit card fraud detection-machine learning methods." 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE, 2019. This research paper focuses on credit card fraud detection using machine learning methods. The authors employ algorithms like Logistic Regression, Random Forest, Naive Bayes, and Multilayer Perceptron on a Credit Card Fraud Detection dataset. The dataset is imbalanced, so oversampling techniques like SMOTE are applied. Feature selection and preprocessing are conducted to enhance model performance. Results show high accuracy for each algorithm, with Random Forest providing the best overall performance. The study highlights the importance of dataset balancing and feature selection in fraud detection. The authors suggest further exploration of algorithms like genetic algorithms and stacked classifiers for improved results. The research is acknowledged to be funded by the SENSIBLE project.

6. Chan, Philip K., et al. "Distributed data mining in credit card fraud detection." IEEE Intelligent Systems and Their Applications 14.6 (1999): 67-74. This research by Philip K. Chan and Salvatore J. Stolfo addresses challenges in credit card fraud detection, where real-world data often has imbalanced class distributions and varying costs for errors. They propose a multi-classifier meta-learning approach that creates subsets with desired class distributions, applies learning algorithms independently and in parallel, and integrates them to optimize cost performance. Empirical results on credit card fraud data show significant reduction in losses due to illegitimate transactions. The approach is scalable and efficient, handling large datasets with skewed distributions and non-uniform error costs. The study emphasizes the impact of training class distribution on classifier performance, providing insights for effective fraud detection systems.

7. Srivastava, Abhinav, et al. "Credit card fraud detection using hidden Markov model." IEEE Transactions on dependable and secure computing 5.1 (2008): 37-48. This paper discusses credit card fraud detection using a Hidden Markov Model (HMM). With the increasing reliance on online shopping and credit card transactions, the risk of fraud has grown. The authors propose using an HMM trained with a cardholder's normal behavior to model the sequence of operations in credit card transactions. If an incoming transaction deviates significantly from the learned behavior, it is flagged as potentially fraudulent. The system focuses on spending patterns, transaction amounts, and other behavioral profiles to detect inconsistencies. The approach is validated through experiments, demonstrating its effectiveness in identifying fraudulent activities. The paper concludes that HMM-based detection can enhance credit card security by alerting users and preventing fraudulent transactions. Future improvements may include algorithm optimization for faster processing and enhanced security measures against potential threats.

8. Ghosh, Sushmito, and Douglas L. Reilly. "Credit card fraud detection with a neural-network." System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on. Vol. 3. IEEE, 1994. This paper discusses the development and implementation of a neural network-based credit card fraud detection system. The authors trained the neural network on a dataset containing labeled credit card transactions, covering various types of fraud such as lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non-received issue (NRI) fraud. The system was tested on a separate dataset, demonstrating significantly improved fraud detection compared to rule-based methods, with fewer false positives. The neural network, implemented at Mellon Bank, showed substantial accuracy and early detection of fraud, outperforming previous detection efforts. The study highlights the importance of using advanced technologies, like neural networks, for effective fraud prevention in the credit card industry.

9. Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning algorithms." Procedia computer science 165 (2019): 631-641. The paper discusses a novel approach for credit card fraud detection using machine learning algorithms. With the rise of online payment modes, the risk of fraud has increased, making it crucial to employ effective detection methods. The proposed method involves clustering cardholders based on transaction amounts, extracting behavioral patterns using a sliding window strategy, and training classifiers on these patterns. The system adapts to changing behaviors through a feedback mechanism to address concept drift. The authors used a European credit card fraud dataset and experimented with various classifiers, emphasizing the Matthews Correlation Coefficient for evaluating

model performance. The results indicate that logistic regression, decision tree, and random forest algorithms performed well, with additional improvements observed after applying the SMOTE technique to address dataset imbalance.

10. Bahnsen, Alejandro Correa, et al. "Feature engineering strategies for credit card fraud detection." *Expert Systems with Applications* 51 (2016): 134-142. This paper addresses the escalating issue of credit card fraud, emphasizing the significance of fraud detection systems in the era of increasing online transactions. Focusing on four main fraud categories within card-not-present transactions, the study employs machine learning models for real-time fraud detection. The evaluation compares various algorithms, considering the skewed distribution of data. The literature review emphasizes challenges in fraud detection, including data sensitivity, imbalance, and adaptability. The experimental methodology involves combining fraud and legitimate transaction logs, data preparation, and applying machine learning models. The study compares and evaluates different models, considering issues like class imbalance. Overall, the research provides insights into optimizing algorithms for detecting specific fraud patterns in credit card transactions.

3. Methodology

3.1 Machine learning:

Machine learning plays a crucial role in identifying and preventing fraudulent transactions within credit card data. The dataset, comprising transactions from September 2013, presents a significant class imbalance, with only 0.172% of transactions labeled as frauds. Traditional accuracy metrics are insufficient due to this imbalance, prompting the use of specialized metrics like the Area Under the Precision-Recall Curve (AUPRC) for evaluation. Machine learning models can leverage numerical input variables, derived through Principal Component Analysis (PCA), to learn patterns indicative of fraudulent activity. The 'Time' and 'Amount' features, which have not undergone PCA transformation, provide additional context to aid in fraud detection. Supervised learning algorithms, such as logistic regression, decision trees, or ensemble methods like random forests, can be trained on this dataset to recognize subtle patterns associated with fraudulent transactions. Feature importance analysis can reveal which components contribute most to fraud detection. Additionally, model deployment can enable real-time monitoring of credit card transactions, automatically flagging or blocking potentially fraudulent activities.

3.2 Dataset:

The dataset for the "Credit Card Fraud Detection" project comprises credit card transactions made by European cardholders in September 2013. It spans two days, encompassing 284,807 transactions, with a highly imbalanced distribution—only 492 of these transactions are identified as fraudulent, constituting a mere 0.172% of the total. The dataset primarily consists of numerical input variables resulting from a Principal Component Analysis (PCA) transformation, preserving only 'Time' and 'Amount' as non-transformed features. 'Time' denotes the seconds elapsed since the first transaction, while 'Amount' signifies the transaction amount. The response variable, 'Class,' assumes a value of 1 for fraudulent transactions and 0 for legitimate ones.

Due to confidentiality concerns, the original features and additional background information are undisclosed. Notably, the imbalanced class ratio necessitates evaluating accuracy using the Area Under the Precision-Recall Curve (AUPRC), as traditional confusion matrix accuracy may be misleading in unbalanced classification scenarios. The project's focus is on developing a robust fraud detection model, taking into account the unique characteristics and challenges posed by the dataset, aiming to enhance the security and reliability of credit card transactions.

3.3 Handling Data Imbalance:

In the context of the "Credit Card Fraud Detection" project, the utilization of SMOTEN (Synthetic Minority Over-sampling Technique for Nominal variables) plays a crucial role in addressing the highly imbalanced nature of the dataset. With only 0.172% of transactions labeled as fraudulent, the dataset presents a significant class imbalance challenge.

SMOTEN is employed as a resampling technique to address this issue by oversampling the minority class (fraudulent transactions) synthetically, generating additional instances to balance the class distribution. Unlike traditional oversampling

methods, SMOTEN considers the nominal nature of categorical variables, ensuring a more accurate representation of the minority class. This is particularly important in fraud detection, where capturing the nuances of fraudulent transactions is critical.

The synthetic generation of minority class instances enhances the model's ability to recognize and distinguish fraudulent patterns, ultimately improving the overall performance of the credit card fraud detection system. The project leverages SMOTEN to enhance the training process and enable the machine learning model to better generalize to rare instances, contributing to the robustness and effectiveness of the fraud detection system in real-world scenarios

3.4 Modeling & Result:

Model	Train accuracy	Train F1 score	Test accuracy	Test F1 score
Decision Tree	1.0	1.0	0.99	0.99
Random forest	1.0	1.0	0.99	0.99
XGBoost	1.0	1.0	0.99	0.99

The credit fraud detection models, including Decision Tree, Random Forest, and XGBoost, demonstrate exceptional performance in accurately identifying fraudulent transactions. The Decision Tree model achieves perfect training accuracy and an impressive test accuracy of 99.95%, along with a corresponding F1 score of 99.95%. This signifies the robustness of the model in distinguishing between genuine and fraudulent transactions.

The Random Forest model, an ensemble of decision trees, exhibits high accuracy and F1 score both in training and testing phases, with values hovering around 99.99%. This ensemble approach contributes to the model's resilience against overfitting, ensuring reliable performance on new data.

XGBoost, a powerful gradient boosting algorithm, achieves perfect training accuracy and an outstanding test accuracy of 99.98%, supported by a matching F1 score. The confusion matrix for XGBoost during training showcases its ability to accurately predict both true positives and true negatives.

These models collectively offer a robust framework for credit fraud detection, showcasing their effectiveness in identifying potentially fraudulent activities while maintaining high accuracy on unseen data. The exceptional performance of these algorithms provides a reliable foundation for implementing fraud detection systems in real-world financial scenarios, emphasizing their significance in safeguarding against fraudulent transactions.

4. Conclusion

The "Credit Card Fraud Detection" project successfully addresses the challenge of imbalanced datasets in fraud detection using machine learning. Leveraging the XGBoost algorithm and resampling techniques like SMOTEN, the project achieves exceptional accuracy and F1 scores, surpassing 99% in identifying fraudulent transactions. The models, including Decision Tree and Random Forest, demonstrate robustness and resilience against overfitting. The emphasis on the Area Under the

Precision-Recall Curve (AUPRC) as an evaluation metric acknowledges the dataset's imbalance, providing a more meaningful assessment of model performance. The real-world implications extend to significant benefits for credit card companies and cardholders, minimizing financial losses and enhancing transaction security. The successful implementation of advanced analytics, specifically XGBoost, showcases the potential of machine learning in mitigating financial risks, establishing a scalable and adaptive framework for cybersecurity challenges. Overall, the project underscores the effectiveness of combining powerful algorithms with thoughtful data handling strategies to create a reliable and efficient credit card fraud detection system.

5. Future Scope

The future scope of the "Credit Card Fraud Detection" project lies in continual refinement and adaptation to evolving cyber threats. Further exploration involves incorporating advanced anomaly detection techniques, leveraging deep learning models for feature extraction, and integrating real-time monitoring systems. Exploring explainable AI methodologies will enhance the interpretability of the models, fostering trust and understanding in their decision-making processes. Additionally, collaboration with financial institutions for access to more diverse and extensive datasets can contribute to model generalization. Incorporating blockchain technology and federated learning may offer enhanced security and privacy in collaborative fraud detection efforts. As the landscape of cyber threats evolves, the project's future work includes the integration of advanced technologies and continuous research to ensure the sustainability and effectiveness of credit card fraud detection systems in the face of emerging challenges.

6. References

- [1] Chaudhary, Khyati, Jyoti Yadav, and Bhawna Mallick. "A review of fraud detection techniques: Credit card." *International Journal of Computer Applications* 45.1 (2012): 39-44.
- [2] Dal Pozzolo, Andrea, et al. "Learned lessons in credit card fraud detection from a practitioner perspective." *Expert systems with applications* 41.10 (2014): 4915-4928.
- [3] Patidar, Raghavendra, and Lokesh Sharma. "Credit card fraud detection using neural network." *International Journal of Soft Computing and Engineering (IJSCE)* 1.32-38 (2011).
- [4] Dal Pozzolo, Andrea, et al. "Credit card fraud detection: a realistic modeling and a novel learning strategy." *IEEE transactions on neural networks and learning systems* 29.8 (2017): 3784-3797.
- [5] Chan, Philip K., et al. "Distributed data mining in credit card fraud detection." *IEEE Intelligent Systems and Their Applications* 14.6 (1999): 67-74.
- [6] Srivastava, Abhinav, et al. "Credit card fraud detection using hidden Markov model." *IEEE Transactions on dependable and secure computing* 5.1 (2008): 37-48.
- [7] Ghosh, Sushmito, and Douglas L. Reilly. "Credit card fraud detection with a neural-network." *System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on*. Vol. 3. IEEE, 1994.
- [8] Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning algorithms." *Procedia computer science* 165 (2019): 631-641.
- [9] Bahnsen, Alejandro Correa, et al. "Feature engineering strategies for credit card fraud detection." *Expert Systems with Applications* 51 (2016): 134-142.
- [10] Varmedja, Dejan, et al. "Credit card fraud detection-machine learning methods." *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 2019.