Credit Card Fraud Detection using Classification Machine Learning and Deep Learning Algorithms

Rim Touny, Sema Mosaad, Nada Zakaria , Dina Mohammady
dept. Electrical and computer engineering
University of Ottawa
Ottawa, Canada
Rim Touny
Nada Zakaria
Sema Mosaad
Dina Mohammady

***Abstract*—Credit card fraud has emerged as a pressing concern for financial institutions and consumers globally, with the rise of digital transactions. The exponential growth of fraudulent activities has resulted in significant financial losses and jeopardized data security. Detecting and preventing credit card fraud in real-time is imperative to safeguard customers from unauthorized charges and preserve the trust of financial systems. In this paper, we present a comprehensive study on credit card fraud detection, leveraging the power of both machine learning and deep learning techniques. Our primary objective is to develop robust and efficient models capable of accurately identifying legitimate and fraudulent transactions, ensuring higher accuracy and precision.**

***Keywords*—Credit Card Fraud Detection, Machine Learning, Deep Learning, Data Science, Classification Algorithms, Principal Component Analysis (PCA), Imbalanced Data, Financial Security.**

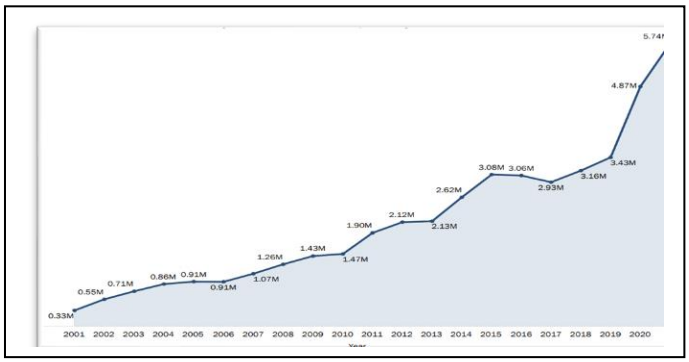
INTRODUCATION

Credit card fraud has become a significant concern for financial institutions and consumers worldwide. With the widespread use of credit cards for transactions, the risk of fraudulent activities has escalated, leading to substantial financial losses and compromised security. Detecting fraudulent transactions in a timely and accurate manner is crucial to protect consumers from unauthorized charges and to maintain the trust and integrity of financial systems.

In this paper, we present a comprehensive study on credit card fraud detection using a combination of machine learning and deep learning techniques. Our primary objective is to develop robust and efficient models that can distinguish between legitimate and fraudulent credit card transactions with high accuracy and precision.

The prevalence of credit card fraud is evident from statistics, with millions of U.S. adults falling victim to credit card fraud annually. As the most common form of identity theft in the United States, it has emerged as a significant challenge for both financial institutions and law enforcement agencies. In 2021 alone, there were millions of reported cases of credit card fraud, further emphasizing the urgency to improve detection and prevention mechanisms.

To conduct our study, we utilize a simulated credit card transaction dataset sourced from Kaggle, covering a period from January 2019 to December 2020. The dataset encompasses a diverse range of legitimate and fraudulent transactions conducted by 1000 customers with a pool of 693 merchants, providing us with valuable insights into transaction patterns and potential fraudulent activities.



Year	# of Reports
2001	325,519
2002	551,622
2003	713,657
2004	860,383
2005	909,314
2006	906,129
2007	1,070,447
2008	1,261,124
2009	1,428,977
2010	1,470,306
2011	1,898,543
2012	2,115,079
2013	2,134,565
2014	2,620,931
2015	3,080,378
2016	3,060,824
2017	2,926,167
2018	3,160,199
2019	3,428,818
2020	4,865,023
2021	5,737,265

Fig. 1. Number of Fraud, Identity Theft and Other Reports by Year in USA.

MOTIVATION

The alarming statistics of credit card fraud cases highlight the urgency of implementing effective fraud detection systems. The increasing number of identity theft reports, accounting for over 40 % of all identity theft cases in the US, and the staggering total of reported fraud incidents in 2021 underscore the importance of proactive fraud prevention. By employing advanced fraud detection techniques, organizations can mitigate financial losses, protect customer trust, and fortify their data security.

System Architecture

A. Introduction

The code begins with a brief introduction, indicating that it is a final project for a Data Science course. It mentions that the project is being conducted in a collaborative environment using Colaboratory, a Google Cloud-based platform for collaborative coding.

B. Set-up Phase

The first phase of the code is the set-up phase. In this phase, the required libraries are installed using pip, and the necessary Python packages for data analysis, visualization, machine learning, and deep learning are imported.

C. Data Loading and Exploration

The code reads the dataset `fraudTrain.csv` using the Pandas library and stores it in a DataFrame called `data`. The initial exploration of the dataset is done using the `head()` method to display the first few rows of the data. Additionally, the code uses the `info()` and `nunique()` methods to get an overview of the data, including the data types, non-null values, and the number of unique values in each column.

D. Data Pre-processing

The data pre-processing phase involves several steps to clean and prepare the data for modeling. These steps include:

1) *Checking for Null Values: The code checks if there are any missing values in the dataset by using the `isnull().sum()` method. This helps to identify columns with missing data, if any.*

2) *Checking for Duplicate Rows: The code uses the `duplicated().sum()` method to determine the number of duplicate rows in the dataset, if any.*

3) *Adding a New Feature 'Age': The code calculates the age of credit card holders based on the 'trans_date_trans_time' and 'dob' columns. This new feature, 'age', is added to the dataset.*

4) *Visualization of Age Distribution: The age distribution of credit card holders is visualized using a kernel density plot, with separate colors for fraud and non-fraud transactions.*

5) *Dropping Unnecessary Features: The code drops certain columns from the dataset that are not required for modeling. These columns include 'Unnamed: 0', 'first', 'last', 'trans_num', and 'cc_num'.*

6) *Correlation Matrix: The correlation matrix is computed to understand the relationships between numerical features. The correlation values are visualized using a heatmap.*

7) *Visualization of Fraud and Non-Fraud Cases: The number of fraud and non-fraud cases is visualized using a bar chart and a pie chart.*

8) *Outlier Detection: Boxplots are used to detect outliers in numerical features. The boxplots are categorized based on fraud and non-fraud cases.*

E. Data Modeling and Prediction

The data modeling phase involves the selection and training of various machine learning classifiers. The code uses different classifiers, such as Support Vector Machine (SVM), Random Forest, Naive Bayes, K Nearest Neighbors (KNN), XGBoost, Stochastic Gradient Descent (SGD), Logistic Regression, Decision Tree, AdaBoost, and CatBoost.

For each classifier, the code performs the following steps:

1) *Data Encoding: The categorical features are encoded using Label Encoding, converting categorical data into numerical format for model training.*

2) *Data OverSampling: To handle class imbalance, the code applies Synthetic Minority Over-sampling Technique (SMOTE) to generate synthetic samples for the minority class (fraud cases).*

3) *Data Scaling: The numerical features are standardized using StandardScaler to bring them to the same scale.*

4) *Splitting Data: The dataset is split into training and testing sets using train_test_split.*

5) *Applying PCA (Principal Component Analysis) or t-SNE: In some cases, the code applies dimensionality reduction techniques like PCA or t-SNE to visualize high-dimensional data.*

6) *Model Training and Evaluation: The classifier is trained on the training set and evaluated on the testing set. The performance metrics, such as accuracy, precision, recall, F1 score, and confusion matrices, are computed and displayed.*

7) *Champion Model Selection: The model with the highest F1 score is selected as the champion model.*

F. Supervised Deep Learning Algorithms

In this section, the code implements deep learning algorithms for fraud detection. Two algorithms are used: Sequential Neural Network (DNN) and Convolutional Neural Network (CNN).

1) *DNN: A DNN with multiple hidden layers is constructed using Keras. The model is trained and evaluated on the data, and classification metrics are computed.*

2) *CNN: A CNN is built using Conv1D and MaxPool1D layers to process the 1D input data.*

The model is trained and evaluated, and the performance is visualized using learning curves.

The code concludes by summarizing the results of the various models and deep learning algorithms used for fraud detection. The champion model is identified based on its performance metrics, and the final evaluation results are presented.

The system architecture consists of data loading, exploration, pre-processing, data modeling using various classifiers and deep learning algorithms, and evaluation of model performance. It aims to provide a comprehensive analysis of credit card fraud detection using a variety of machine learning and deep learning techniques.

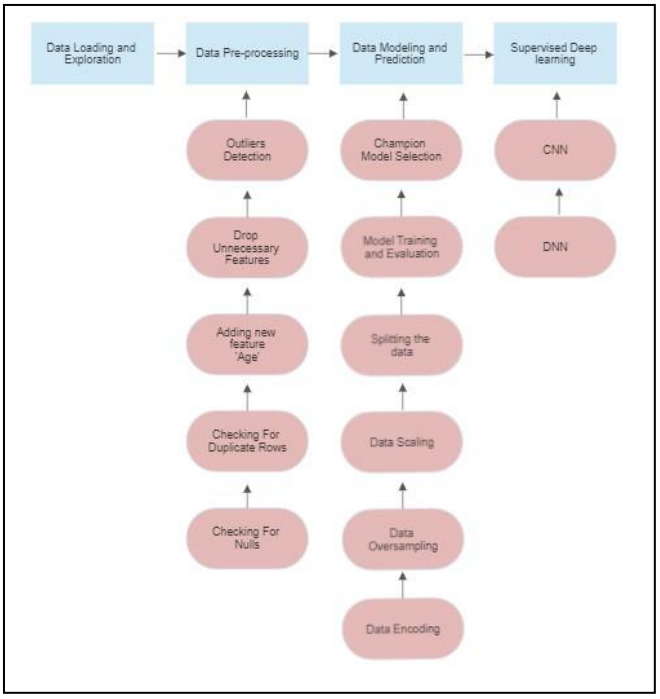


Fig. 2. Data Flow Diagram

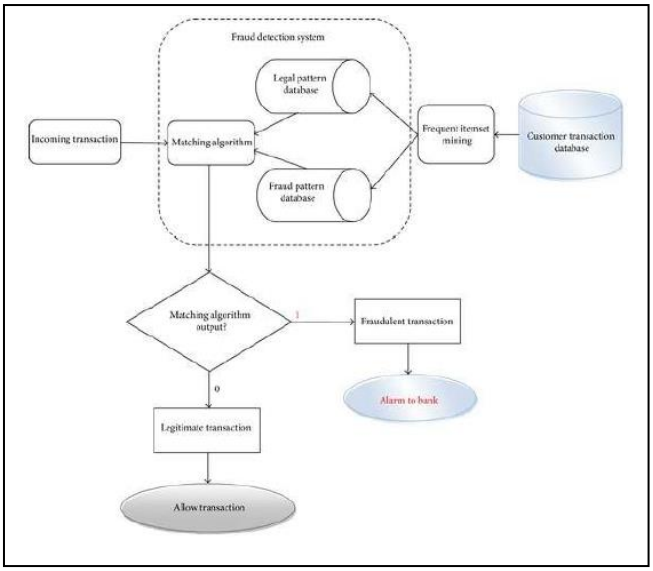


Fig. 3. System Architecture

MODEL

The model for credit card fraud detection is a crucial component of the system architecture. It is responsible for processing credit card transaction data, classifying transactions as legitimate or fraudulent, and providing accurate predictions in real-time. In this section, we will elaborate on the models used in the credit card fraud detection project.

A. ***Classification Algorithms:*** *The project explores various classification algorithms to identify the most effective one for fraud detection. The following algorithms are considered:*

1) *XGBoost (Extreme Gradient Boosting): XGBoost is an ensemble learning method that utilizes gradient boosting to create a powerful predictive model. It is known for its efficiency and high performance in handling large datasets, making it suitable for credit card fraud detection.*

2) *Random Forest: Random Forest is an ensemble learning method that creates multiple decision trees and combines their predictions to obtain more accurate and robust results. It excels in handling imbalanced datasets and has strong generalization capabilitie*

3) *Decision Tree Classifier: Decision trees are simple yet effective models that recursively split the data into branches based on feature values. Decision Tree Classifier is easy to interpret and provides insights*

4) *K Nearest Neighbors (KNN): KNN is a non-parametric algorithm that classifies new data points based on the majority class of their K-nearest neighbors. It is suitable for detecting fraud patterns that are localized or clustered in the feature space.*

5) *Support Vector Machine (SVM): SVM is a powerful algorithm for both classification and regression tasks. It finds the optimal hyperplane that best separates data points of different classes. SVM is effective in high-dimensional spaces and can handle non-linear decision boundaries with the use of kernel functions.*

6) *Gaussian Naive Bayes: Naive Bayes is a probabilistic algorithm based on Bayes' theorem with the assumption of feature independence. Gaussian Naive Bayes specifically assumes that numerical features follow a Gaussian distribution.*

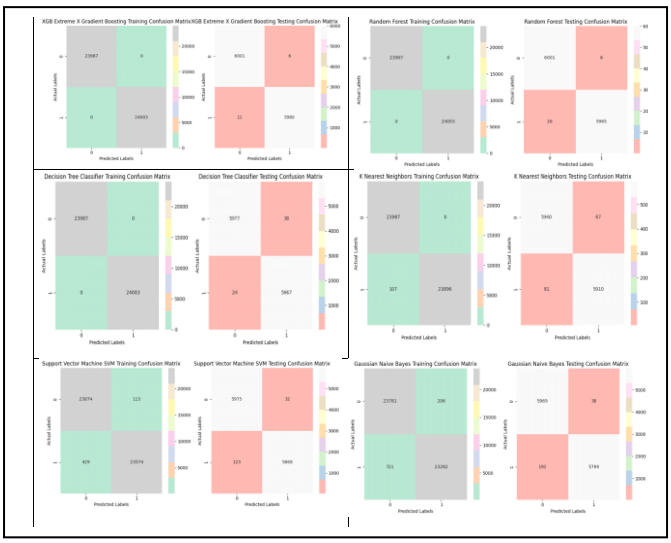


Fig. 4. Confusion Marric for each Classifications Algorithms (Testing/Training)

B. ***Deep Learning Algorithms:*** In addition to traditional machine learning algorithms, the project explores deep learning techniques for credit card fraud detection:

1) *Sequential Model in Keras: A sequential model is a linear stack of layers in Keras, a high-level neural network API. The model is composed of input, hidden, and output layers, and it is trained using backpropagation. This model can handle sequential data and is well-suited for fraud detection tasks.*

2) *Convolutional Neural Network (CNN): CNNs are primarily used for computer vision tasks, but in this project, they are applied to credit card fraud detection. CNNs are designed to automatically learn hierarchical patterns and features from raw input data, making them effective at processing large datasets like credit card transactions.*

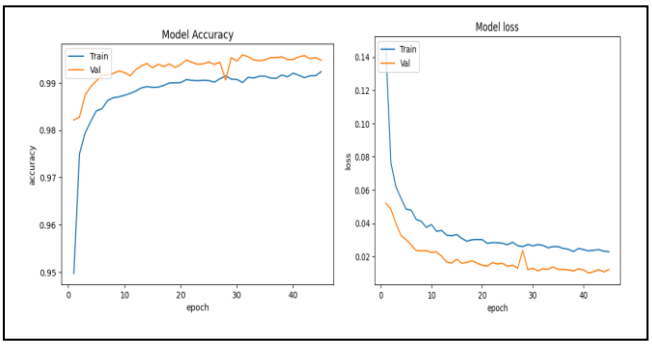


Fig. 5. Model loos and Model Accuarcy

Adding MaxPool

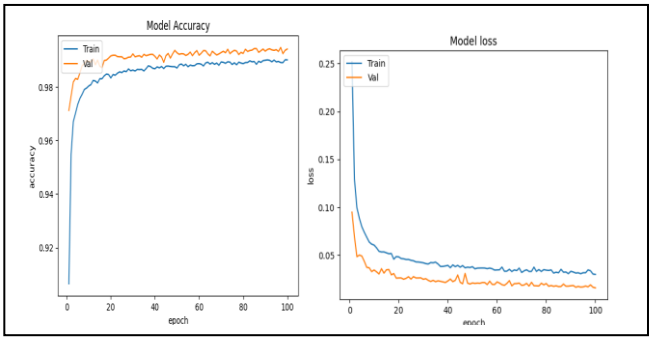


Fig. 6. Model Accuarcy and Model loss after adding MaxPool

PERFORMANCE EVALUATION

The evaluation section of the paper presents the performance of various classification algorithms for credit card fraud detection, measured using the F1 score. The F1 score is a suitable metric for imbalanced datasets, where fraudulent transactions are rare compared to legitimate ones.

- When PCA was used for dimensionality reduction, the F1 scores for all algorithms dropped significantly.

	F1 score	Accuracy	Precision	Recall
Random Forest	0.711776	0.715619	0.720540	0.703221
XGB Extreme X Gradient Boosting	0.696179	0.699117	0.702088	0.690369
Decision Tree Classifier	0.674475	0.675696	0.676115	0.672843
K Nearest Neighbors	0.621209	0.681447	0.764577	0.523118
Gaussian Naive Bayes	0.548823	0.527088	0.524070	0.576031
Support Vector Machine SVM	0.501198	0.531672	0.535267	0.471207

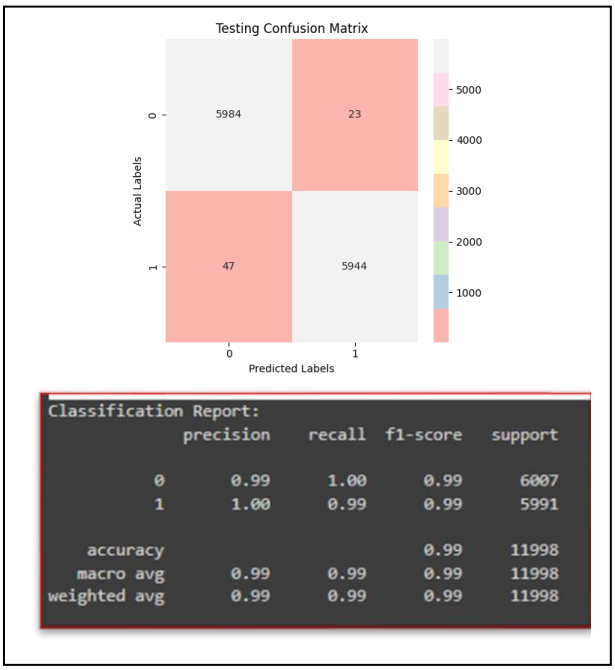
Fig. 7. Model Evaluation using PCA

- However, Without using PCA, the F1 scores for different algorithms are quite high, indicating their effectiveness in detecting fraudulent transactions.

	F1 score	Accuracy	Precision	Recall
XGB Extreme X Gradient Boosting	0.998581	0.998583	0.998998	0.998164
Random Forest	0.997325	0.997333	0.998995	0.995660
Decision Tree Classifier	0.995495	0.995499	0.994997	0.995994
K Nearest Neighbors	0.987634	0.987665	0.988790	0.986480
Support Vector Machine SVM	0.986965	0.987081	0.994576	0.979469
Gaussian Naive Bayes	0.980555	0.980830	0.993490	0.967952

Fig. 8. Model Evaluation without using PCA

- The Deep Learning Algorithms, represented by a sequential model in Keras and a Convolutional Neural Network (CNN),achieved remarkable F1 scores of 0.99. The classification report shows high precision, recall, and F1-score for both class 0 (legitimate transactions) and class 1 (fraudulent transactions), indicating the models' ability to effectively distinguish between the two classes



Classification Report:

	precision	recall	f1-score	support
0	0.99	1.00	0.99	6007
1	1.00	0.99	0.99	5991
accuracy			0.99	11998
macro avg	0.99	0.99	0.99	11998
weighted avg	0.99	0.99	0.99	11998

Fig. 9. Deep Learning Algothrims Evalution

In summary, the evaluation demonstrates that without PCA, traditional machine learning algorithms, especially XGBoost and Random Forest, achieved excellent performance in credit card fraud detection. However, when PCA was used for dimensionality reduction, there was a noticeable drop in the algorithms' effectiveness. On the other hand, the Deep Learning Algorithms, including the sequential model in Keras and CNN, achieved consistently high F1 scores, showcasing their potential for accurate fraud detection. Overall, the evaluation provides valuable insights into the models' performance, aiding in selecting the best-performing model for real-world credit card fraud detection applications.

SUMMARY AND CONCLUSION

In conclusion, this paper demonstrates the significance of data science and machine learning in addressing the critical issue of credit card fraud detection. The project's methodology covers various essential steps, from data exploration and preprocessing to model training and evaluation. The exploration of multiple classification algorithms helps identify the best-performing models, such as XGBoost and Random Forest, which are highly effective in detecting fraudulent transactions.

The study also showcases the promising application of deep learning algorithms, including the sequential model in Keras and CNN, in credit card fraud detection. These deep learning models achieve consistently high F1 scores, reflecting their ability to learn complex patterns and features from raw transaction data.

The evaluation results provide valuable insights into the strengths and limitations of different models, guiding the selection of the most appropriate model for deployment in the production environment. Continuous monitoring and updating of the model are essential to adapt to evolving fraud patterns and maintain optimal performance.

Overall, this paper contributes to the growing field of credit card fraud detection, emphasizing the importance of data science and machine learning in mitigating financial risks, protecting consumers, and maintaining the integrity of credit card transactions. By adopting the best-performing models and incorporating deep learning techniques, financial institutions can enhance their fraud detection capabilities and foster a safer and more secure environment for credit card transactions. Future work can focus on continuous feature engineering, data augmentation, real-time monitoring, and collaboration with other institutions to collectively improve fraud detection across the industry.

REFERENCES

[1] Kaggle|Credit Card Fraud Detection DataSet

[2] J. C. Mathew, B. Nithya, C. R. Vishwanatha, P. Shetty, H. Priya and G. Kavya, "An Analysis on Fraud Detection in Credit Card Transactions using Machine Learning Techniques," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 265-272, doi: 10.1109/ICAIS53314.2022.9742830.

[3] Li, Y., Chen, X., Luo, Y., Zhang, T., & Yang, J. (2020). Credit Card Fraud Detection Based on Improved XGBoost Algorithm. Security and Communication Networks, 2020, 1-9.

[4] Patil, A. D., & Bhosale, U. B. (2020). Credit Card Fraud Detection Using Machine Learning: Comparative Study. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1-5). IEEE.

[5] Patil, A. D., & Bhosale, U. B. (2020). Credit Card Fraud Detection Using Machine Learning: Comparative Study. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1-5). IEEE.