# CREDIT CARD FRAUD DETECTION USING STATE-OF-THE ART MACHINE LEARNING ALGORITHMS

**Dr.K.MAHESH[1], B.NANDINI[2], M.SAHITH REDDY[2], K.BHAGEERADHA[2]**

*[1] Associate Professor, [2] Student, B. Tech, Department of CSE (AI&ML), CMR Technical Campus,Kandlakoya(V), Medchal Road, Hyderabad - 501401*

## ABSTRACT

The topic outlines the pervasive issue of credit card fraud within the financial sector, emphasizing its detrimental effects on both financial institutions and consumer confidence. Traditional rule-based systems are deemed inadequate in addressing the evolving tactics employed by fraudsters, necessitating more sophisticated approaches. Consequently, the primary objective of the study is to develop a fraud detection system that is both robust and efficient. This entails accurately identifying fraudulent transactions while minimizing false positives, thereby enhancing the overall security and integrity of the financial system. To achieve this goal, the researchers utilize a large dataset containing labeled credit card transactions, encompassing both legitimate and fraudulent instances, for training and evaluation purposes. The methodology employed involves feature engineering, wherein relevant information is extracted from the transactional data, followed by the selection and optimization of machine learning models. Several state-of-the-art algorithms, such as Random Forest, Gradient Boosting, Support Vector Machines, and Neural Networks, are evaluated to determine the most effective model for detecting fraud. By employing this comprehensive approach, the study aims to contribute to the development of more effective fraud detection mechanisms, thereby mitigating financial losses and bolstering consumer trust in the financial industry.

Keywords: Credit Card Fraud, Machine Learning algorithms, Client, Labeled Credit Card Transactions.

## 1. INTRODUCTION

This discusses credit card fraud (CCF), which is a form of identity theft where unauthorized transactions are made using someone else's credit card or account information. It highlights that credit cards that have been stolen, lost, or counterfeited are often used for fraudulent activities. This mentions a specific type of credit card fraud known as card-not-present fraud, which occurs when a credit card number is used for online or remote transactions where the physical card is not required. With the rise of e-commerce and online shopping, card-not-present fraud has become increasingly prevalent. Furthermore, this notes that the expansion of e-banking and various online payment platforms has created more opportunities for fraudsters to carry out credit card fraud. This has led to significant financial losses, amounting to billions of dollars annually, as fraudsters exploit vulnerabilities in these digital environments to perpetrate their crimes. Overall, this underscores the growing threat of credit card fraud, fueled by advancements in technology and the increasing reliance on digital payment methods, and highlights the importance of implementing robust security measures to combat this pervasive issue.

## 2. RELATED WORK

The previous survey highlights the challenges of credit card fraud detection in the electronic payment world. It focuses on using data-driven methods, specifically machine learning, to address these complexities. The paper emphasizes two key aspects:

Understanding the Fundamentals: It starts by explaining the typical credit card fraud detection setup, including the type of data used (dataset and its attributes), how performance is measured (metrics), and how to handle imbalanced datasets (where fraudulent transactions are much rarer than legitimate ones). These fundamentals are crucial for tackling any credit card fraud detection problem.

Adapting to Change: The paper then dives into a specific challenge - dataset shift, also known as concept drift. This refers to the situation where the patterns in fraudulent activity change over time. The machine learning models need to adapt to this evolving landscape to stay effective in detecting fraud.

## 3. PROPOSED WORK

The system outlined here tackles credit card fraud using a two-pronged approach: powerful machine learning models and in-depth feature engineering. For the machine learning models, they'll leverage algorithms like Random Forest, Gradient Boosting, Support Vector Machines (SVMs), and Neural Networks. These are known for their ability to learn intricate patterns from data. This is crucial since fraudsters employ ever-evolving tactics. By using these models, the system can continuously learn and adapt to identify new fraudulent activities, improving overall detection accuracy. However, the raw transaction data itself might not be enough. To empower the machine learning models, feature engineering comes into play. This involves extracting and crafting specific characteristics (features) from the data that are most informative for fraud detection.

Firstly, the system incorporates various machine learning algorithms known for their effectiveness in handling complex data and detecting subtle patterns indicative of fraudulent activity. These include Random Forest, Gradient Boosting, Support Vector Machines (SVM), and Neural Networks. Each algorithm offers unique strengths in learning from data and identifying fraudulent transactions. For instance, Random Forest excels in handling high-dimensional data and mitigating overfitting, while Gradient Boosting focuses on iteratively improving model performance by minimizing errors.

Secondly, the system employs advanced feature engineering techniques to extract pertinent information from transactional data. This involves the creation of additional features beyond raw data inputs to enhance the discriminative power of the machine learning models. These features may include temporal aspects such as time of day or day of the week, transaction sequences to identify patterns in consecutive transactions, customer behavior patterns to differentiate between normal and suspicious behavior, and anomaly detection features to flag unusual activities.

### 3.1 NAVIE BAYES

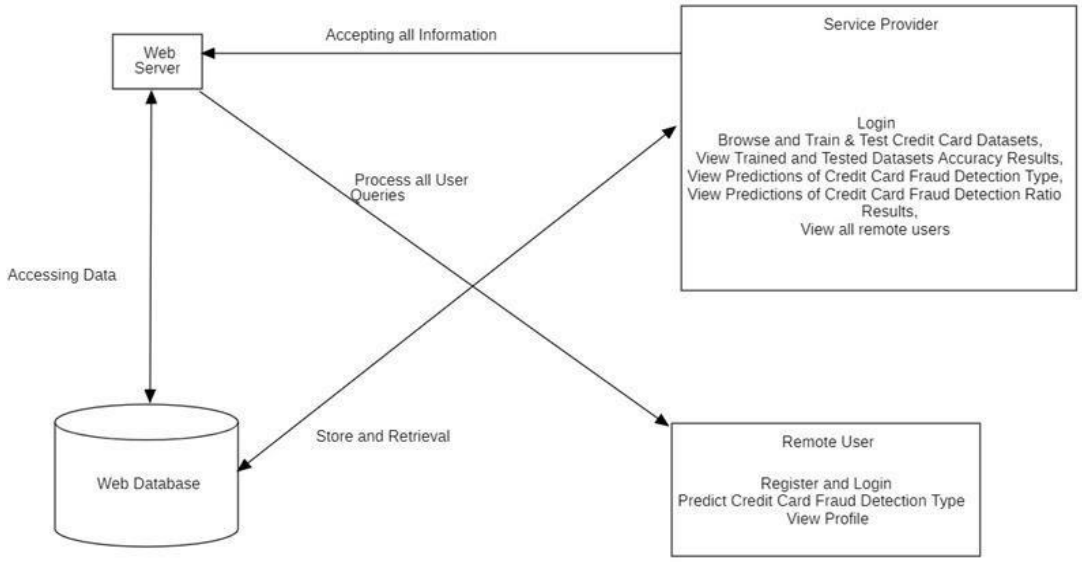
The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature. Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias). While the Naive Bayes classifier is widely used in the research world, it is not widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they do not understand the interest of such a technique.

### 3.2 DECISION TREE CLASSIFIER

Decision tree classifiers are used successfully in many diverse areas. Their most important feature is the capability of capturing descriptive decision-making knowledge from the supplied data. Decision tree can be generated from training sets. Decision trees are often used in conjunction with other techniques. For instance, they might be employed for initial fraud screening, and then more complex models can be used for further analysis of flagged transactions. Overall, decision trees offer a valuable tool in the credit card fraud detection toolbox, especially for interpretability and handling imbalanced datasets. However, decision trees also have limitations. They can be prone to overfitting, where the model performs well on the training data but struggles with unseen data. Additionally, they might not capture complex relationships between features as effectively as some other models.

3.3 SUPPORT VECTOR MACHINE

In classification tasks a discriminant machine learning technique aims at finding, based on an independent and identically distributed (iid) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point x and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to genetic algorithms (GAs) or perceptron's, both of which are widely used for classification in machine learning.




## 4. EXPERIMENTAL SETUP AND DATASET

### 4.1 EXPERIMENTAL SETUP

The project "CREDIT CARD FRAUD DETECTION USING STATE-OF-ART MACHINE LEARNING" needs specific hardware and software components Hardware Requirements: These define the minimum computer components needed. It specifies a processor of i5 or higher, at least 4GB of RAM, and 20GB of hard disk space. A standard Windows keyboard, a two- or three-button mouse, and an SVGA monitor are sufficient. Software Requirements: These outline the necessary software programs to operate the system. The operating system needs to be Windows 7 or later. The code will be written in Python, a popular programming language for data science. For the user interface, it will use a combination of HTML, CSS, and JavaScript. On the backend, Django-ORM, a Python framework, will facilitate interaction with the database. MySQL will serve as the database management system to store the data. Finally, Wamp server, a software package, will provide the environment to run the web application.

DATASET

The credit card dataset is accessible for research purposes. The dataset [11] holds transactions made by a cardholder over a two-day period, i.e., September 2018. There were 284,807 transactions in total, of which 492, or 0.172 percent, were fraudulent. Because disclosing a consumers transaction details is considered a problem of con identicality, the main component analysis is applied to the majority of the datasets features using principal component analysis (PCA). PCA is a standard and widely used technique in the relevant literature for reducing the dimensionality of such datasets, increasing interpretability but at the same time minimizing information loss. It contains only numerical input variables which are the result of a PCA transformation. Unfortunately, due to confidentiality

issues, we cannot provide the original features and more background information about the data. Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependent cost-sensitive learning.

## 5 RESULTS AND DISCUSSION

The bar graph you sent appears to be comparing the performance of various machine learning algorithms for credit card fraud detection. Here's a breakdown of what the graph likely shows, based on the labels:

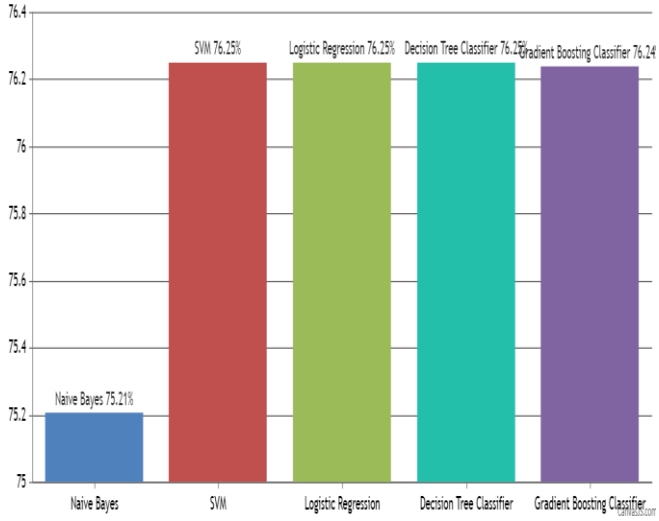
The x-axis lists five different machine learning algorithms: Naive Bayes, Support Vector Machine (SVM), Logistic Regression, Decision Tree Classifier, and Gradient Boosting Classifier.

The y-axis shows the percentage of correctly identified fraudulent transactions, possibly measured by accuracy or AUC (Area Under the Curve). All the algorithms have a detection rate above 75%.

The heights of the bars represent the performance of each algorithm. Here's a descending order of performance, based on the graph:

SVM and Logistic Regression (tied at around 76.25%)
Decision Tree Classifier (around 76.24%)
Gradient Boosting Classifier (around 76.2%)
Naive Bayes (around 75.2%)

Without knowing the specific dataset used to train these models, it's difficult to say definitively which algorithm is the best. However, the graph suggests that SVM and Logistic Regression might be the most performant in this particular scenario for credit card fraud detection. It's important to note that this is just a single comparison, and the best model for a real-world application can depend on various factors like the specific dataset, computational resources, and desired balance between accuracy and other metrics.




## 6 CONCLUSION AND FUTURE SCOPE

### 6.1 CONCLUSION

This highlights the escalating threat of credit card fraud to financial institutions, driven by fraudsters' persistent efforts to devise new methods. It underscores the importance of deploying a robust classifier capable of adapting to the evolving nature of fraud. The primary objective of a fraud detection system is accurately predicting fraud cases while minimizing false positives, as these instances can lead to inconvenience and mistrust among legitimate customers. Furthermore, this emphasizes that the performance of machine learning (ML) methods in detecting credit card fraud can vary depending on the specific business case. Factors such as the type of input data play a crucial role in determining which ML methods are most effective. For instance, certain algorithms may excel

when dealing with high-dimensional data with numerous features, while others may be better suited for datasets with a large number of transactions. Moreover, this suggests that key factors influencing the performance of ML models in credit card fraud detection include the number of features, the volume of transactions, and the correlation between these features.

## 6.2 FUTURE SCOPE

This outlines the promising future of credit card fraud detection, emphasizing the advancements expected through cutting-edge machine learning methodologies. One significant development foreseen is the evolution of deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs). These sophisticated models are anticipated to provide more precise and resource-efficient fraud detection systems by leveraging their ability to capture complex patterns and relationships within data. CNNs excel at extracting spatial features, while RNNs are adept at modeling sequential data, making them well-suited for analyzing transactional information in credit card data. Additionally, this highlights the integration of explainable AI (XAI) techniques into these advanced models. This integration aims to enhance transparency and interpretability, which are crucial for building trust and understanding the decision-making process behind fraud alerts. By providing insights into how the models arrive at their conclusions, XAI techniques can help financial institutions and regulatory bodies better comprehend and validate the outputs of fraud detection systems. Another frontier in credit card fraud detection is the development of real-time fraud detection mechanisms. As transactions occur rapidly in electronic payment systems, there is a growing need for systems capable of swiftly identifying and preventing fraudulent activities as they happen. Advancements in stream processing and rapid inference algorithms are expected to play a key role in enabling real-time fraud detection.

## REFERENCES

[1] Y. Abakarim, M. Lahby, and A. Attius, ``An efficient real time model for credit card fraud detection based on deep learning," in *Proc. 12th Int. Conf. Intell. Systems: Theories Appl.*, Oct. 2018, pp. 1_7, Doi: 10.1145/3289402.3289530.

[2] H. Abdi and L. J. Williams, ``Principal component analysis," *Wiley Inter- disciple. Rev., Computer. Statist.*, vol. 2, no. 4, pp. 433_459, Jul. 2010, Doi: 10.1002/wics.101.

[3] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ``Facilitating user authorization from imbalanced data logs of credit cards using altricial intelligence," *Mobile Inf. Syst.*, vol. 2020, pp. 1_13, Oct. 2020, Doi: 10.1155/2020/8885269.

[4] A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ``Performance analysis of feature selection methods in software defect prediction: A search method approach," *Appl. Sci.*, vol. 9, no. 13, p. 2764, Jul. 2019, Doi: 10.3390/app9132764.

[5] B. Bandaranayake, Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia, J. Cases Educ. Leadership, vol. 17, no. 4, pp. 3453, Dec. 2014, doi: 10.1177/1555458914549669.

[6] J. Baszczy ski, A. T. de Almeida Filho, A. Matuszyk, M. Szelg, and R. Sowi ski, Auto loan fraud detection using dominance-based rough set approach versus machine learning methods, Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[7] https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023