**CREDIT CARD FRAUD DETECTION USING A HYBRID MACHINE LEARNING ALGORITHM**

*Shubham Singh a\*,Rahul Neware*

*a School of Computer Science, Vellore Institute of Technology, Bhopal-466114, India*

**Abstract**

The usage of Internet banking and credit cards is growing at an exponential rate. As more people use credit cards, online banking, and debit cards, the probability of becoming a victim of fraud of various kinds also increases. In recent times, there have been a number of instances in which credit card company users have, due to a lack of understanding, given their card information, personal information, and one-time password to an unidentified fraudulent caller. Credit card fraud is a major problem for both consumers and financial institutions. It can lead to significant financial losses, as well as damage to the reputation of the financial institution. Many different methods can be used to detect credit card fraud, but one of the most effective is machine learning. Machine learning algorithms can be trained on historical data to identify patterns and anomalies that are indicative of fraud. In this paper, we review the state-of-the-art in machine learning for credit card fraud detection. In the past, there have been many studies on the same topic using many famous machine-learning methods. But here we will see how good hybrid machine learning does on the same problem statement, with an understanding of the concept of hybrid machine learning.

**Introduction**

Since the beginning of the digital process, there have always been individuals who are looking for new methods to get unauthorized access to the financial information of another person. Due to the fact that all purchases can now be readily performed online by just inputting the credit card details, this has developed into a significant concern in the current day. Credit card fraud is a major problem for both consumers and financial institutions. It can lead to significant financial losses, as well as damage to the reputation of the financial institution Credit card fraud is a growing problem, with losses totaling billions of dollars each year. Fraudsters are constantly developing new methods to steal credit card information and commit fraud, making it increasingly difficult for financial institutions to detect and prevent fraud.

Moving with the facts, According to The Nilson Report [nila], the losses due to credit card, debit card, and prepaid card fraud reached $16.31B worldwide in 2015. And the recent report by The Nilson Report [nila] shows that the gross fraud loss reached $22.8B in 2018, which is 4% more than that in 2015 and is expected to exceed by an even more significant amount in the coming years. According to Statista [sta], the gross fraud reached $5.6B in 2012, whereas in 2018, the fraud loss reached $9.1B, which is approximately two-fifths of the total loss. In particular, 70% of these frauds are Card-Not-Present (CNP) frauds (i.e., frauds conducted online or over the telephone), 20% are counterfeits and the remaining 10% cases are related to losses due to lost cards.

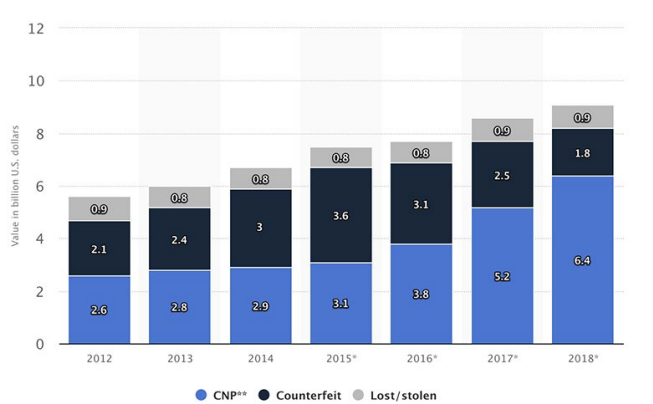


Fig1.1 Graph showing the number of cases of credit card fraud

Increased credit card usage has also been accompanied by increased credit card fraud or scams. A report released by the National Crime Records Bureau (NCRB) shows that 3,432 cases of debit and credit card fraud in India were registered in 2021, an increase of nearly 20% from 2020.

In 2021, the Federal Trade Commission (FTC) fielded nearly 390,000 reports of credit card fraud, making it one of the most common kinds of fraud in the U.S. But that figure doesn’t begin to offer a complete view of the problem.

In December 2022, the Nilson Report, which monitors the payments industry, released a forecast indicating that U.S. losses from card fraud will total $165.1 billion over the next 10 years, plaguing every age group in every state. Just one type of credit card fraud — card-not-present fraud, which involves online, over-the-phone and mail-order transactions — accounted for an estimated $5.72 billion in U.S. losses in 2022, according to Insider Intelligence.

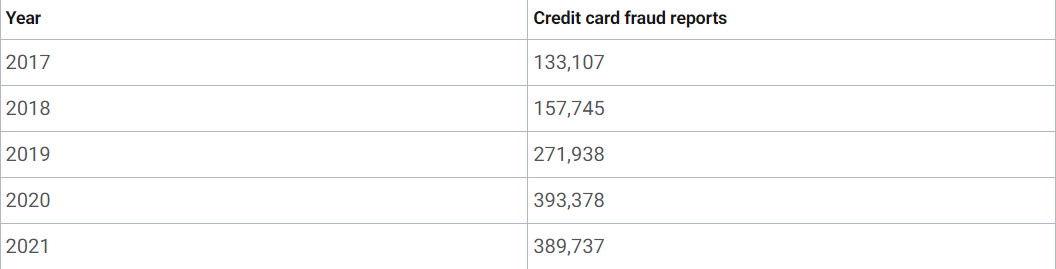


Fig 1.2: credit card Fraud Reports from the year 2017 to 2021

Credit Card Fraud Detection with Machine Learning is an approach that takes the data investigation by a team of Data Scientists as well as model development, which will give the best outcomes in preventing revealing and fraudulent transactions. This process can be thought of as a hybrid between traditional data analysis and artificial intelligence. This is accomplished by combining all of the important aspects of the transactions made by card users, such as Client Behavioral Patterns, Provider, Amount, Product Category, User Zone, Date, and so on. Clone transactions have been used to make transactions that are close to the original one or to replicate a transaction. This may occur when an organization sends an identical invoice to various departments within a partner company in an attempt to get payment from that partner on many occasions. When a system is able to differentiate between a transaction that was done in mistake and one that was fraudulent, then that is the best choice. Now after enlisting all the important aspects, we have to decide the methods we will use for the predictions. In these aspects, there can be some parameters which are categorical type data [now when you have categorical data the methods, we can use Linear Decent Analysis, Random Forest method, SVM, Decision Tree, logistic regression, CNN model, gradient boosting] and there can be other parameters which can be numerical type data [now the numerical data is good for regression models like SVM, Linear regression, Logistic regression, Decision Trees, Random Forest, Gradient Boosting and CNN]. In this context, the adoption of some Machine Learning techniques which are capable of working with both categorical and numerical data would be more effective in distinguishing clone transactions produced by human mistake from actual fraudulent activity will be chosen to make the hybrid machine learning models. Here in this paper, we will understand the concepts of hybrid machine learning with its advantages and will make a hybrid model to demonstrate a better performance than any other single model.

**Literature review**

In this section, we will be sharing and discussing different Machine Learning Methods which we will apply to the same topic of credit card fraud detection. We will go through some of such past experiments in which different models like Random Forest, Decision Trees, SVM, Logistic Regression, Gradient boosting, and deep learning CNN models will be used for the Fraud prediction. Here I will study and try to understand the work done on these models with the problem and accuracy it will return on the credit card fraud detection. By understanding issues and recording the best accuracies we will decide the model we will be using for the hybrid modeling. So, this literature review examines the methods and strategies employed in credit card fraud detection, providing insights into the strengths and weaknesses of different ML approaches and after that taking the best out of them for hybrid modeling.

1. **Decision Tree:**

The decision tree technique is proposed as a statistical data mining technique that expresses independent and dependent attributes logically in the form of a tree structure. Decision trees divide large problems into several basic ones and solve them through iteration.

The Decision Tree model is divided into two stages based on credit card fraud detection. The first stage involves creating a decision tree using available training data and applying decision rules to classify incoming transactions. The MLPC method is used as pre-pruning, stopping the tree's growth at the pruning level selected before construction.

The figure below shows the confusion matrix of prediction results obtained by applying a decision tree algorithm of machine learning. In this, you can see that the decision tree algorithm is correctly predicting zeros in the final output 94739.0 times and incorrectly predicting zeros 30.0 times. The decision tree algorithm makes 130 accurate predictions and 37 incorrect predictions.

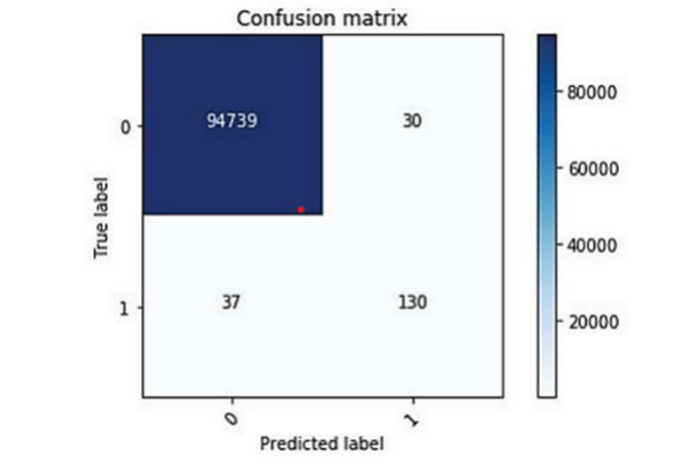


Fig .1: Confusion matrix for decision tree.

**2. Random Forest Technique:**

Credit card fraud detection using the Random Forest machine learning method is an effective approach. This technique employs a Random Forest classification algorithm, which is a supervised learning method utilizing decision trees for dataset classification. Random Forest is known for its robustness and ability to handle complex data.

In practice, a dataset containing information about credit card transactions is collected and preprocessed. Relevant features are selected and transformed, and the Random Forest model is trained on this data. The model learns to distinguish between normal and fraudulent transactions, making it a valuable tool for fraud detection.

One significant advantage of Random Forest is its ability to handle large and diverse datasets, providing good predictive accuracy. The model used to detect fraud in credit cards using Random Forest, this model scored 99.908% in accuracy. Additionally, it can adapt to evolving fraud patterns, making it a valuable asset for financial institutions in the ongoing battle against credit card fraud.



Fig 2: python code for Random Forest technique.

**3. Logistic Regression:**

The model used to detect fraud in credit cards using Logistic Regression, this model scored 97.2% in accuracy, 97% sensitivity, and 2.8% Error Rate.

Logistic regression is a statistical model that can be used to predict the probability of a binary outcome, such as yes or no, true or false, or 1 or 0. It is a type of supervised machine learning algorithm, which means that it is trained on a dataset of labeled examples, where the input variables are known and the output variable is the binary outcome that we want to predict the fraud in credit card where we can take the fraud as 1 and not fraud as 0.

Logistic regression is a widely used algorithm in machine learning and statistics. It is relatively simple to understand and implement, and it can be used to solve a wide variety of problems such as credit card fraud detection.

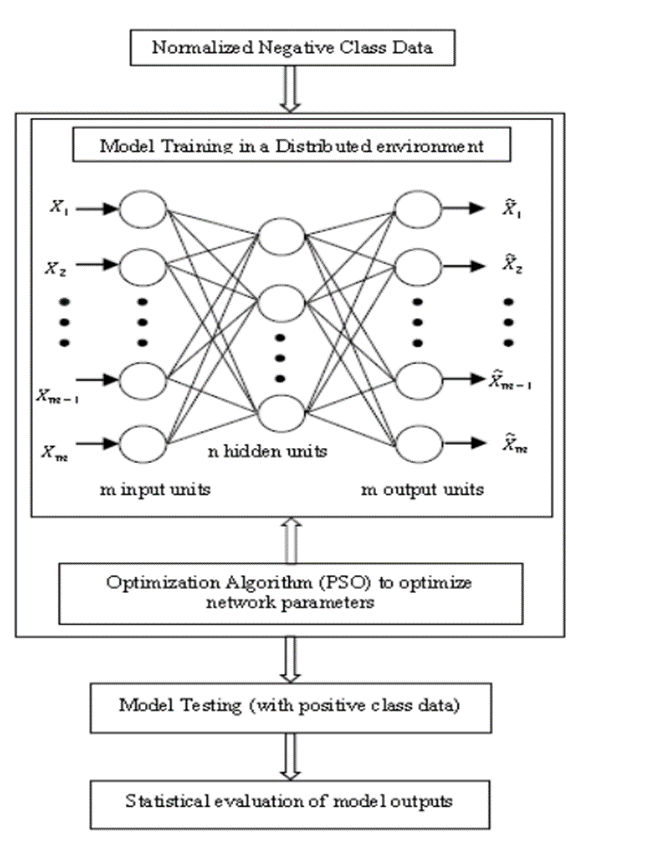


Fig 3: Training Model for Logistic Regression.

Accuracy is the overall number of instances that are predicted correctly to detect credit card fraud, accuracies are represented by a confusion matrix that shows the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). True Positive represents the transactions that are fraudulent and were correctly classified by the model as fraudulent. True Negative represents the not fraudulent transactions that were correctly predicted by the model as not fraudulent. The third rating is False positive which represents the transaction that is fraudulent but was misclassified as not fraudulent. And finally, False Negatives which are not fraudulent transactions.

Accuracy = (TP+TN)/(TP+TN+FP+FN)

Accuracy For Logistic Regression = 97.2%

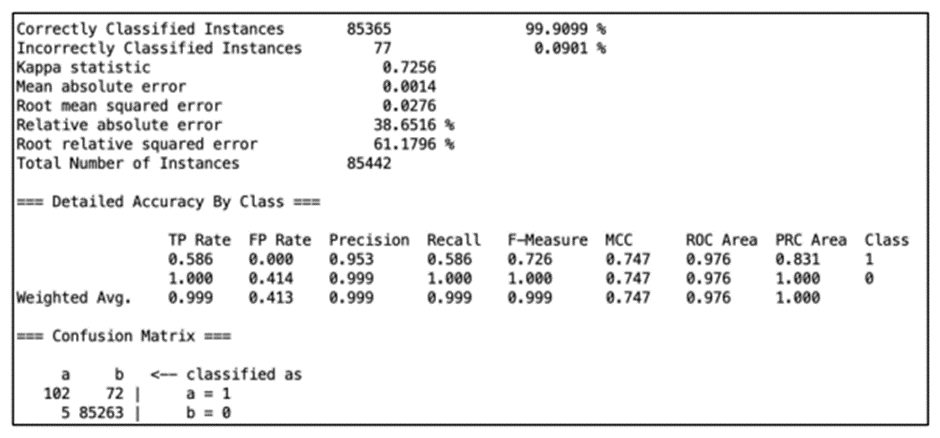


Fig 4: Accuracy for Logistic Regression.

**4. Gradient Boosting:**

Gradient boosting is a machine learning technique that combines multiple weak models, like decision trees, to create a strong predictive model. It's an iterative process where each model corrects the mistakes made by the previous ones. The process continues until a stopping criterion is met or the desired level of accuracy is achieved. They've been successfully applied in various domains, including credit card fraud detection and we will go through the reason why if effective also.

Gradient boosting algorithms are ideal for credit card fraud detection due to their versatility as both regressors and classifiers. They train models by reducing the differential loss function using gradient descent optimization, improving model accuracy and reducing bias error. It can handle categorical data directly without converting them into numerical values, which is beneficial for credit card fraud detection. They also have built-in features to address common fraud detection challenges, such as overfitting and target leakage. It uses a permutation-based approach on different data subsets for training, preventing overfitting and target leakage issues.

Overall, gradient boosting algorithms are chosen for credit card fraud detection due to their high accuracy, effective handling of categorical data, and mitigation of common fraud detection challenges.

For classification and regression issues, a powerful method called the gradient boosting classifier can be used. Gradient boosting models can perform quite well on very complex datasets, but they are also prone to overfitting, which can be prevented in a number of ways

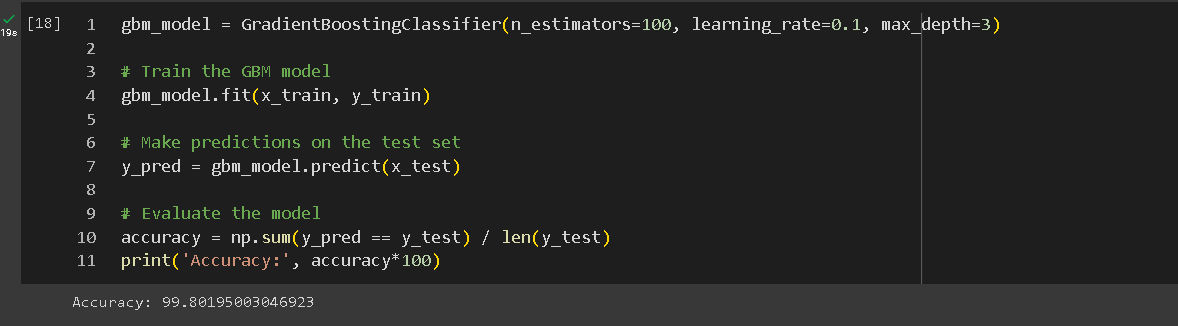


Fig 5: python code for Gradient Boosting.

The precision rate is 99.801%, showcasing the excellent performance of gradient boosting algorithms in accurately detecting fraudulent credit card transactions.

**5. Support Vector Machine Model:**

Detecting credit card fraud is vital in the financial industry to minimize losses for both institutions and cardholders. SVM, a robust binary classification method, is gaining traction as an effective tool to address this issue. SVM's ability to handle categorical data enhances its real-world application.

Our algorithm outlines a structured process for SVM-based credit card fraud detection, covering data preprocessing, feature transformation, model training, evaluation, and prediction. This systematic approach streamlines the creation of a reliable fraud detection system.

SVM-based credit card fraud detection consistently delivers impressive results. With an accuracy rate of 95.99% and strong precision, recall, and F1-score values, SVM excels at distinguishing fraudulent from legitimate transactions. When adapted as gradient boosting applications, Support Vector Machines offer a compelling solution, preventing overfitting and ensuring accurate results. The proposed algorithm presents a structured framework for implementing SVM-based fraud detection, promising high accuracy and robust performance.

**6. Convolution Neural Network:**

Mrs. M. Madhavi, and K.R.Venkat Reddy, have done their investigation with different calculations pointing towards the aim of using CNN  (convolution layer) which Extracts all important features for credit card fraud detection. For this, they trained a model and tested that model which included:

Step 1 – Collection of the data from different sites like kaggle.

Step 2 – Applying the Data Pre-processing steps.

 Step 3 – Applying the SMOTE Oversampling technique.

Step 4 – Applying the CNN Algorithm. Step 5 – Calculate the score to get a good model.

They train a CNN model as a convolutional neural network (CNN) is a deep learning algorithm that is particularly well-suited for problems where the model itself understands and makes the feature parameter from the given dataset. They used it because CNNs are a powerful tool for credit card fraud detection because they can learn complex patterns from data, are robust to overfitting, and can be used to detect fraud in real time.

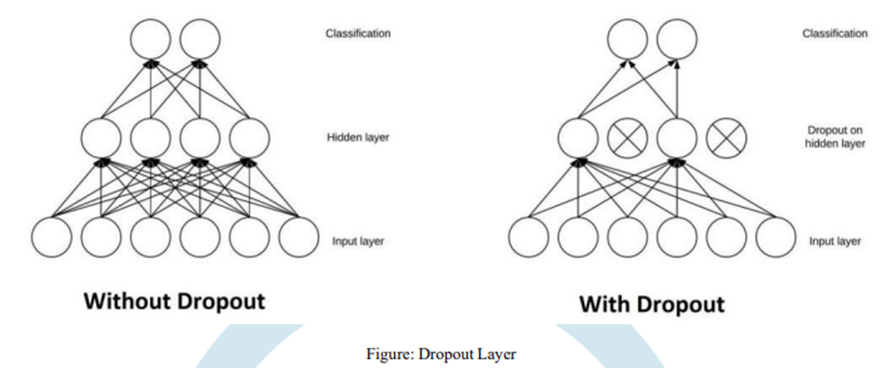


Fig 6: Dropout Layer.

CNN training process using two convolution layers. The first layer contains 32 filters with a kernel size of 3 and uses the relu activation function. The second layer has 64 filters with a kernel size of 3 and uses the relu activation function. The input shape is changed from 2D to 3D. A pooling layer with a max pool size of 2 is used, followed by a flatten layer that transforms the pooled feature map into a one-dimensional vector. This output is fed into the dense layer, which uses the relu activation function and the units of 64. The output is then fed into the dropout layer, which nullifies some neurons' contributions to the next layer. Dropout layers are crucial in training CNNs to prevent overfitting and prevent learning of features only appearing in later samples or batches. The output layer is the output layer.

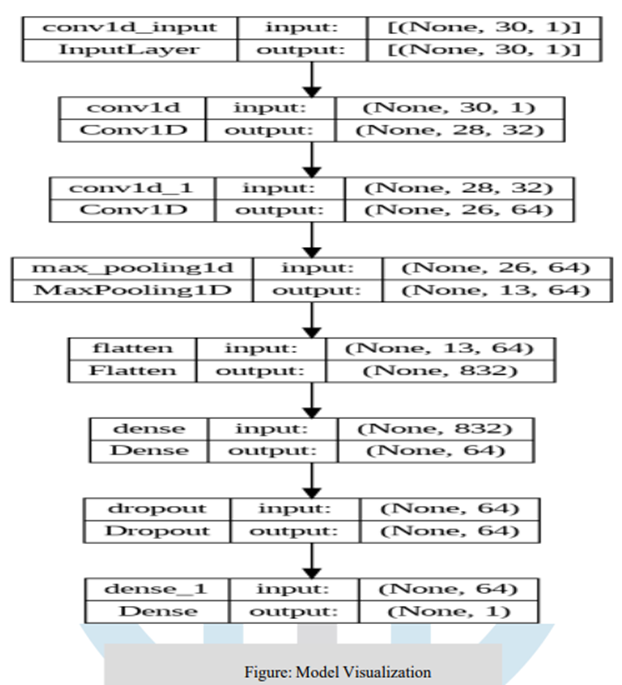


Fig 7: Convolutional Neural Network (CNN) Diagram.

The below diagram will show the model architecture for the model trained:

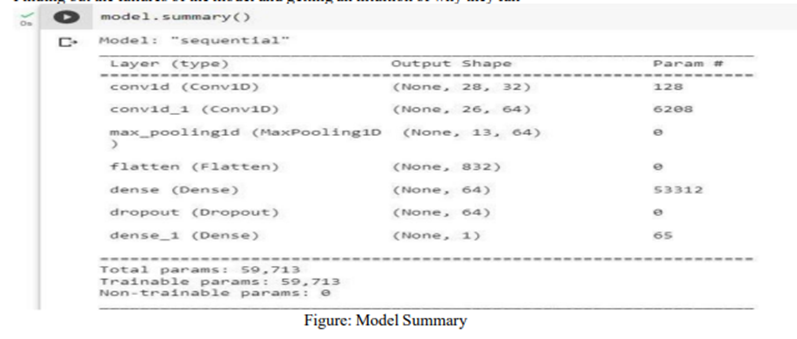


Fig 8: Convolutional Neural Network (CNN) architecture.

From this, they got an accuracy of 99.901 and a training loss of 0.34.

**Literature Review Conclusion**

In conclusion, our literature review has provided valuable insights into various machine learning models used for credit card fraud detection. We have observed a range of accuracy rates among these models, with Convolutional Neural Networks (CNN) demonstrating the highest accuracy at an impressive 99.901%. Other models, such as Logistic Regression and Support Vector Machine, have also shown strong performance, achieving accuracies of 97.2% and 95.99%, respectively. Decision Tree models, while still effective, exhibited slightly lower accuracies at 95% and 94%, respectively.

| Model | Accuracy |
| --- | --- |
| Gradient Boosting | 99.801% |
| Support Vector Machine Model | 95.99% |
| Logistic Regression Model | 97.2% |
| Decision Tree Model | 94% |
| Convolutional Neural Networks (CNN) Model | 99.901% |
| Random Forest Model | 99.908 % |

Table 1: Accuracy table for respective models.

After looking at the table we can see the Random Forest, gradient boosting model, and the CNN model have the highest accuracy. Now we will be using these methods to frame our hybrid model so that we can come up with a model that performs better than any other methods.

**Hybrid Machine Learning**

**What is a Hybrid Machine Learning Algorithm?**

Hybrid machine learning combines different approaches such as supervised and unsupervised learning, reinforcement learning, or deep learning to address complex problems. It can help to overcome the limitations of individual machine learning algorithms. Hybrid machine-learning architectures can combine the strengths of different machine-learning algorithms to overcome these limitations. It allows for a more comprehensive analysis of data and can lead to more accurate predictions or insights. Hybrid machine learning can be used to solve a wide variety of machine learning problems. It is a powerful tool for improving the performance, efficiency, and interpretability of machine learning models. However, it is important to carefully consider the specific needs of your problem and the challenges of hybrid machine learning before using them.

**Why Hybrid Architecture is Effective for Credit Card Fraud Detection?**

Hybrid architectures are well-suited for credit card fraud detection because they can be easily updated to adapt to new fraud patterns. This is important because credit card fraudsters are constantly developing new techniques to avoid detection.

Hybrid architectures can frequently outperform normal machine learning techniques or deep learning algorithms. This is because hybrid architectures can use the strengths of several machine learning methods to overcome their limitations.

When working with huge datasets, hybrid architectures can be more efficient, because hybrid architecture can break the problem into smaller subtasks, which can then be solved by individual machine learning algorithms that are more efficient for particular tasks.

Hybrid architectures can be more interpretable. This is because normal machine learning algorithms are often easier to interpret than deep learning algorithms. By combining a deep learning model with a traditional machine learning algorithm, it is possible to create a hybrid architecture that is both accurate and interpretable.

**Hybrid Machine Learning for fraudulent detection**

Now we have gone through all the points and aspects to make a hybrid model for fraud detection. So now, we will step by step make our model and taking all the essential step required:

* **Data Source:**

The dataset was retrieved from an open-source website, Kaggle.com. It contains data of transactions that were made in 2013 by credit card users in Europe, in two days only. The dataset consists of 31 attributes, 284,808 rows. 28 attributes are numeric variables that due to confidentiality and privacy of the customers have been transformed using PCA transformation, the three remaining attributes are “Time” which contains the elapsed seconds between the first and other transactions of each attribute, “Amount” is the amount of each transaction, and the final attribute “Class” which contains binary variables where “1” is a case of fraudulent transaction, and “0” is not as case of fraudulent transaction. Dataset Link: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>.

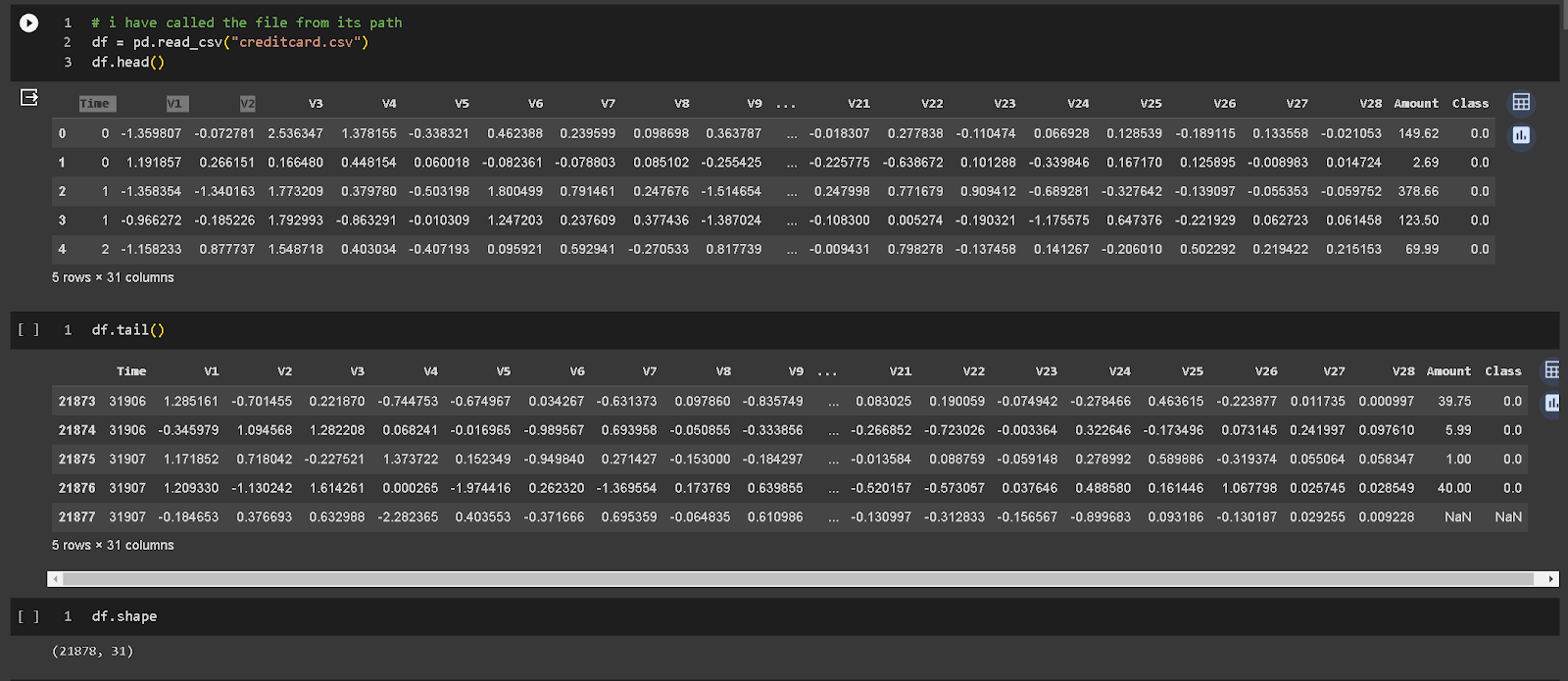
* **Data Analysis and Processing:**

Before starting the programming of model, it’s important that you check or analyze data so that you

can remove any null value or unexpected values and errors. This is an important a step because the

data we acquire could have these errors and it is important to remove it else the model will give errors. In this analyzation:

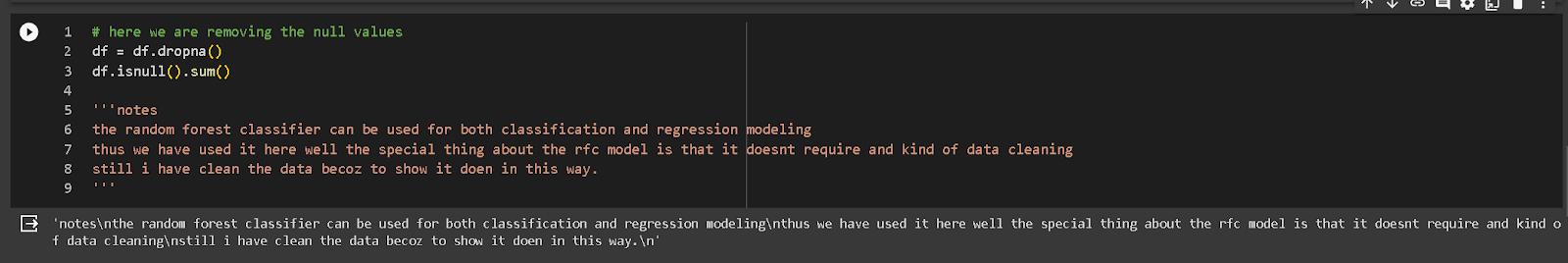
1. Checking the data set to know the form of data entries and the number of row and column:



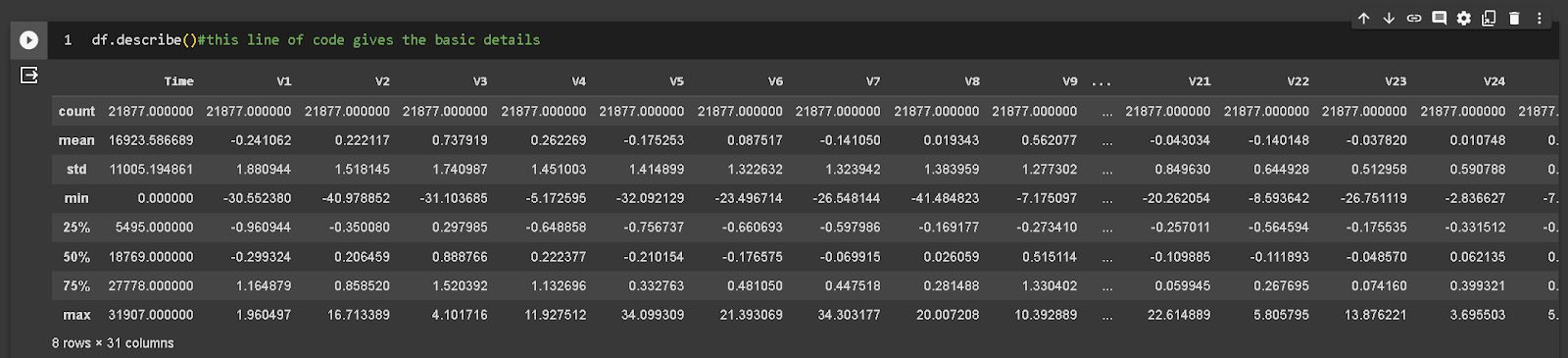
1. Checking whether the entries are empty or null, thus entries can lead to errors as such data couldn’t be processed by the mode. In such cases, the empty entries are filled with synthetic values or by removing the null value row. Here for this data set we will drop the null values:



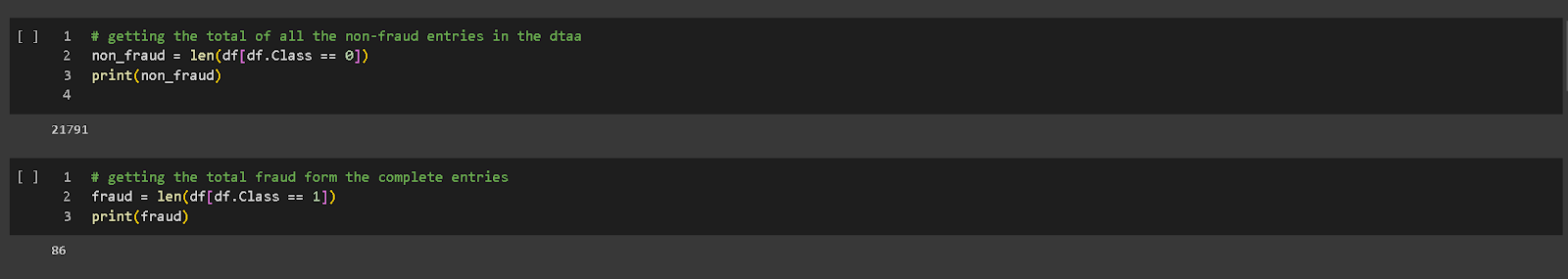
Here, in the above image, only ‘Amount’ and ‘Class’ are having 1 in front of them showing that there is only 1 null entry. Now to remove it we will use the drop method:



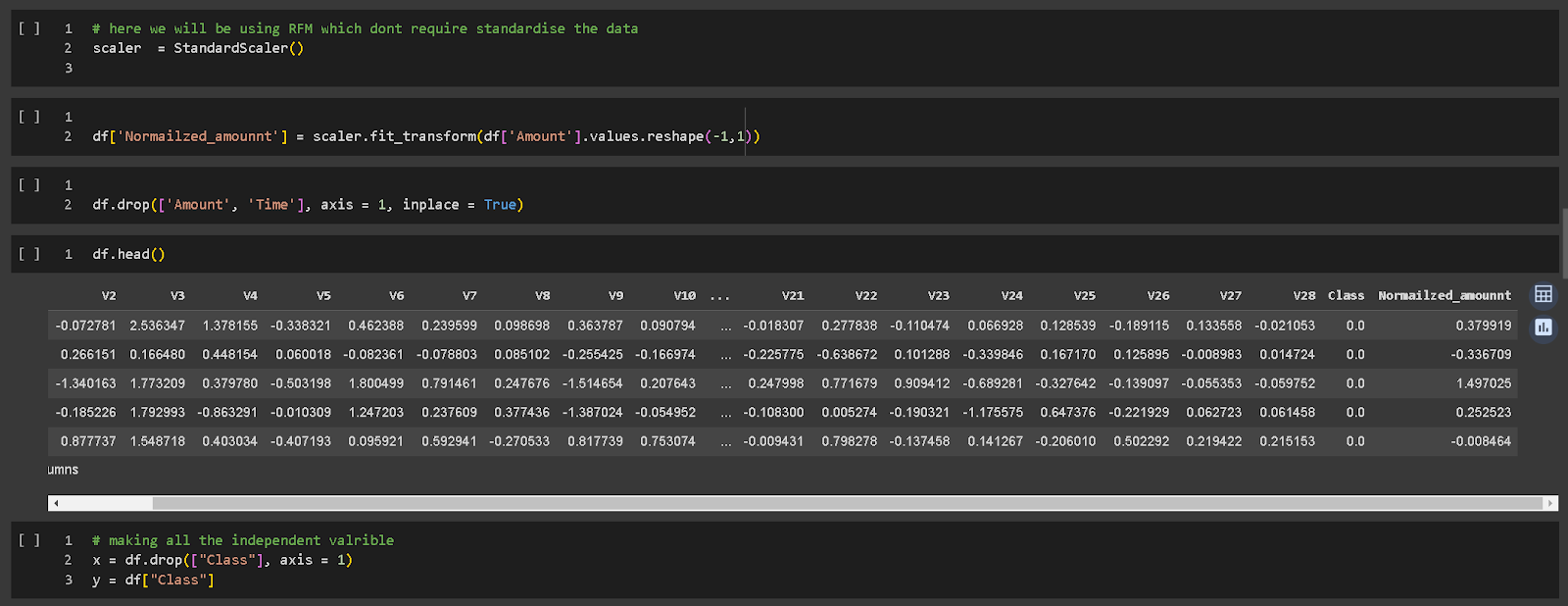
1. Using describe function we will obtain the basic description about the data:



1. Getting the count of fraud count and non fraud count in the Class column:

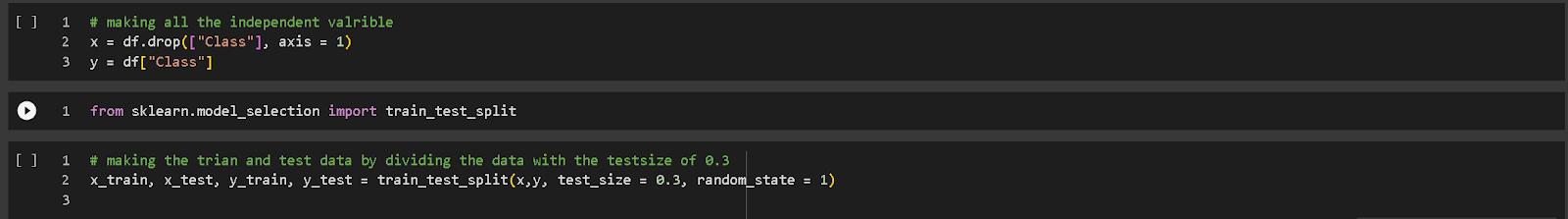


1. Normalizing the values which are varied from the range other columns are present.



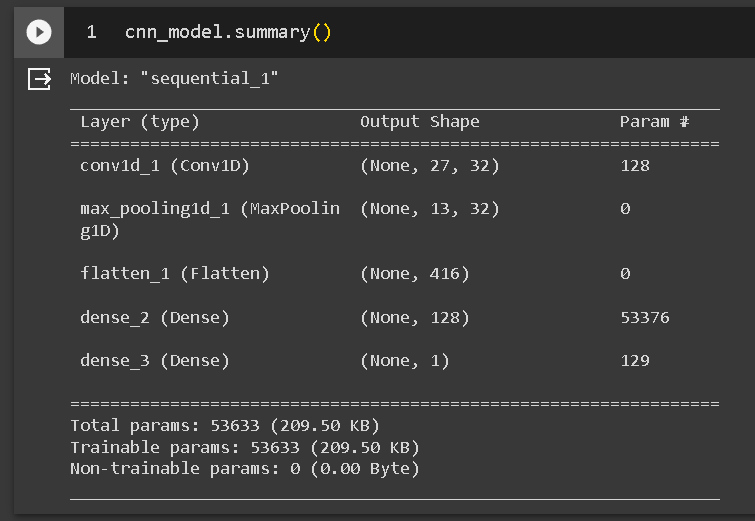
* **Data Modeling:**

In this part, data will be divided into dependable and independent parts namely “y” and “x” respectively. After this we will use these “x”(independent data) and “y”(dependent data) data to split into train and test subjects in the ratio of 3:10. We will be doing this modeling using the scikit learn python lib. :

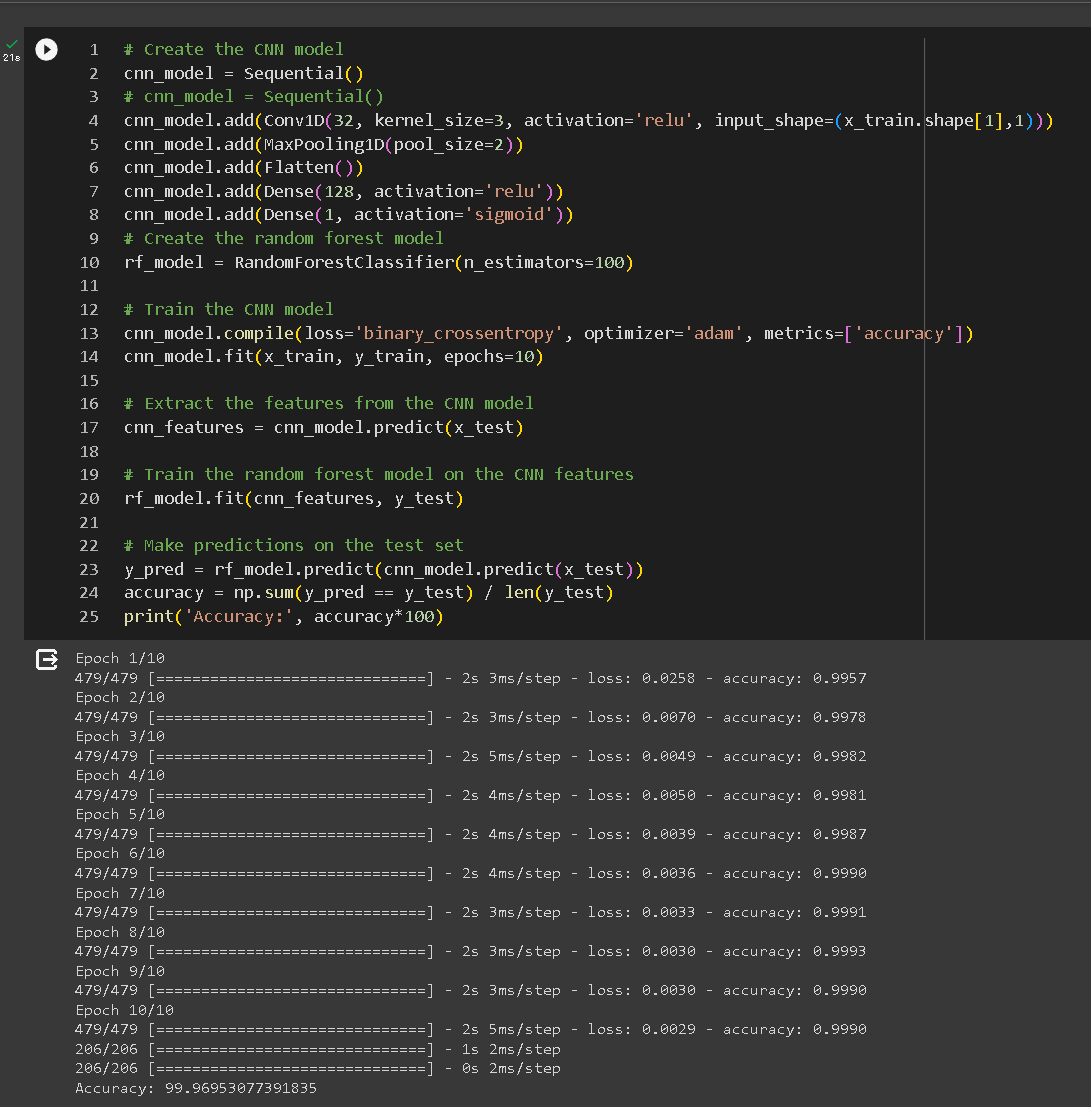


* **Hybrid model making:**

Here we will be making a hybrid model using the random forest method and CNN model, as these have the best accuracy when performed individually. By making a hybrid model we will try to overcome the flaws these two models have in them. Here in this model, we will combine a random forest of 100 trees and CNN with the configuration of :



We used the libraries of TensorFlow for making CNN like Dense, Conv1D, MaxPooling1D, and Flatten. Whereas we used scikit learn libraries to model the random forest model.



**Conclusion**

So now on comparing, you can see the hybrid model (accuracy of 99.97%) performed much better than the other machine learning methods(highest accuracy was 99.908%). Now our work was not just to show that the hybrid model works on a particular dataset h, But we can conclude that for this problem statement, the Hybrid model will always work better. As datasets related to this problem statement will always be solved using classification models and regression models, thus CNN and random forest model is best to use for hybrid model. From this, we conclude that the hybrid model will be the best option for credit card fraud detection.

**References**

1. Kumar, Sheo & Gunjan, Vinit & Ansari, Mohd Dilshad & Pathak, Rashmi. (2022). Credit Card Fraud Detection Using Support Vector Machine. 10.1007/978-981-16-6407-6\_3.
2. Sai Kiran, Jyoti Guru, Rishabh Kumar, Naveen Kumar, Deepak Katariya, Maheshwar Sharma (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. International Journal of Advance Research, Ideas and Innovations in Technology, 4(3) [www.IJARIIT.com](https://www.ijariit.com/).
3. Mohammed, Emad, and Behrouz Far. “Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study.” IEEE Annals of the History of Computing, IEEE, 1 July 2018, doi.ieeecomputersociety.org/10.1109/IRI.2018.00025.
4. Randhawa, Kuldeep, et al. “Credit Card Fraud Detection Using AdaBoost and Majority Voting.” IEEE Access, vol. 6, 2018, pp. 14277–14284., doi:10.1109/access.2018.2806420.
5. <https://link.springer.com/chapter/10.1007/978-981-16-3675-2_40>
6. <https://www.grafos.cl/Articulos/HandwritingAnalysisforDetectionofPersonalityTraitsusingMachineLearningApproach.pdf>
7. <https://thesai.org/Downloads/Volume11No12/Paper_65-Fraud_Detection_in_Credit_Cards.pdf>
8. <https://www.webology.org/data-cms/articles/20220922064230pmPaper103.pdf>
9. <https://www.ijrti.org/papers/IJRTI2304141.pdf>
10. <https://www.researchgate.net/publication/357728400_Credit_Card_Fraud_Detection_Using_Support_Vector_Machine>
11. <https://bard.google.com/chat>
12. https://chat.openai.com/