# An Approach to Detect Credit Card Fraud Utilizing Machine Learning

**Anik Malaker**
Department of Computer Science, American International University Bangladesh
Email: anik.partho555@gmail.com
**Abid Hasan Miad**
Department of Computer Science, American International University Bangladesh
Email: abidhasanmiad@gmail.com
**Farzana Karim Mim**
Department of Computer Science, American International University Bangladesh
Email: farzana.mim8008@gmail.com
**Walid Bin Wahid Badhan**
Department of Computer Science, American International University Bangladesh
Email: walidbadhan94@gmail.com
**MD. ISMAIL HOSSEN***
Department of Computer Science, American International University Bangladesh
Email: ismail.hossen@aiub.edu

## ABSTRACT

With the increasing popularity of Credit card usage, Credit Card fraud also increases. The number of online payment options has expanded thanks to e-commerce and several other websites, raising the possibility of online fraud. As a result, both people and financial institutions suffer significant losses. This research seeks to detect credit card fraud and make attempts to cut down on it. Financial institutions place a high priority on identifying and stopping fraudulent activity. Fraud prevention and detection are pricey, time-consuming, and labor-intensive processes. Several machine-learning algorithms can be utilized for detection. In order to evaluate past customer transaction information and identify behavioral traits, the study's main goal is to develop and apply a special fraud detection algorithm for simulcasting transaction data. Through the research, try to give a genuine solution to Credit card users and make their transactions secure. This research aims to propose a trustworthy and efficient way for identifying credit card fraud. The accuracy of several autonomous classifiers using machine learning that were employed for recognition is compared and examined. The Random Forest classifier has the highest accuracy of 99.98%.

Keywords – **Credit card fraud, Neural network, Random Forest, Imbalanced classification, Machine learning.**

Date of Submission: November 13, 2022 Date of Acceptance: December 20,2022

## I. INTRODUCTION

The fraudulent use of payment cards, such as credit or debit cards, is referred to as "credit card fraud" in general. Payments to a different account under the criminal's control or the acquisition of goods or services could be the motive. With rising fraud in government agencies, courts, the financial sector, the corporate sector, and many other institutions, credit card fraud is a significant threat today. The unlawful use of a credit card account by someone other than the account owner is known as credit card transaction fraud. The issue of credit card fraud now affects every country and every nation. Fraud with a credit card is against the law. Both financial institutions and people suffer significant losses as a result. Many financial institutions and banks are concerned about fraud detection as this crime costs them about $67 billion annually.[12] As a result, financial institutions place a high priority on the detection and prevention of fraudulent operations. Due to our heavy reliance on the internet, the percentage of credit card fraud incidents has increased, but fraud has increased both online and offline. As a result, we believe we have aspirations to finish fraud detection. The only way to cut down on these costs is to use effective machine learning (ML) algorithms to identify fraud, which is an innovative technique to cut down on credit card fraud. There are several sorts of fraud, including securities fraud, credit card fraud, statement fraud, and insurance fraud. Credit card fraud is the most typical sort of all of them. It is described as the usage of a credit card account without authorization. It happens when the cardholder and card issuer are unaware that a third party is using the card. Depending on the characteristics of the fraudulent acts, credit card fraud is divided into many categories. Here is a little introduction to them.

- Offline fraud: The simplest kind of credit card theft involves a stolen card. Additionally, it is the quickest to be found.
- Application fraud: When people use fraudulent personal information to apply for new credit cards.
- Bankruptcy fraud: This entails using a credit card while bankrupt and making purchases while being aware that one will not be able to pay.
- Internal fraud: When bank staff utilize the card information remotely by stealing the card data.
- Counterfeit fraud: When transactions are done remotely, the cardholder is not required to be present; all that is required are the specifics of an authorized credit card. Skimming or shoulder surfing can be used to access the card's information.

Credit card databases provide details on individual transactions, including account number, card type, kind of purchase, place and time of transaction, client's name, merchant code, transaction value, etc. ML algorithms can identify fraud and atypical credit card transactions. Collecting and organizing the raw data is the first and most important phase, after which the model is trained to forecast the possibility of fraud. Four classification techniques—Decision Tree, Random Forest, K-nearest neighbors and Naive Bayes were combined in this research. These algorithms for classification are frequently employed to solve issues. We compare them using the same training dataset as a result. The end result may also include a cross-sectional comparison with other recent investigations.

## II. **Literature Review**

The authors of [1] proposed development inside the overall performance of credit card fraud detection with the aid of using growing diverse strategies which can be primarily based totally on signal processing. Improving the schooling of detectors is the important purpose of this approach. The surrogate samples are generated from authentic fraud samples in this mechanism. The variance of the estimate is decreased right here such that the schooling of detectors may be improved. Due to the presence of diverse issues and the regular extrusion of styles gifts inside the information flow, it's far more important to offer a dependable augmentation of the goal-scarce populace of frauds. The actual information turned into used on this test to illustrate the abilities of proposed strategies such that the overall performance of detection may be improved.

[2] The fraudulent transactions may be detected via way of means of utilizing both this sort or integrating any of those methods. The version can study in a greater correct way via way of means of including new features. Several data mining strategies are being utilized by financial institutions and credit score card organizations for detecting fraud behaviors. The ordinary utilization sample of customers relying upon their beyond sports may be recognized via way of means of making use of any of those methods. Therefore, a comparative evaluation is made right here via way of means of analyzing exclusive fraud detection strategies proposed over the years.

The authors of [3] supplied a look at the normally observed crime inside the credit score card applications. There are sure troubles confronted while the existing non-information mining processes are carried out to keep away from identification theft. A novel information mining layer of protection is proposed for fixing those troubles. For detecting fraud inside diverse applications, several algorithms: RF, DT, DS, RT, NN, LR, DL. There is a huge moving window, better numbers of attributes, and several hyperlinks sort to be had which may be searched through CD and SD algorithms. Thus, consequences may be generated through the machine by eating a massive quantity of time. Since the attackers do now no longer get time to adjust their behaviors with recognition to the algorithms being deployed in actual time, there is no proper assessment executed even after everyday replacement of the algorithms. Therefore, it is not feasible to well exhibit the idea of adaptability. These troubles may be resolved by making sure upgrades inside the proposed set of rules in destiny work.

[4] Research that evaluates the effectiveness of various algorithms after it has been applied to credit card fraud records is extremely skewed. The 284,807 transactions from European cardholders were utilized as a source to create the dataset of credit card transactions. A hybrid method of under-sampling and over-sampling is used on the skewed records. In Python, there are 4 unique methodologies that are used on raw and preprocessed data: The performances of various strategies are assessed based on specific criteria such

as precision, sensitivity, accuracy, balanced class charge, and so forth. The results of the actual execution show that KNN performs better overall when comparing naive Bayes and logistic regression techniques.

[5] The three main categories of fraud—insurance, corporate, and bank—were taken into consideration when they conducted a study on the detection of credit card fraud. Focus on the following two categories of credit card transactions: Physical and virtual. They concentrated on data mining, decision trees, fuzzy logic-based systems, support vector machines, neural networks, artificial immune systems, k-nearest neighbors, naive Bayes, genetic algorithms, regression, classification, logistic regression, and other topics. In which they provided theoretical background on six data mining techniques, including classification, clustering, prediction, outlier identification, regression, and visualization. The current statistical and computational techniques are then described, including the Artificial Immune System, Bayesian Belief Network, NN, LR, SVM, Trees, Self-Organizing Maps, and Hybrid Methods. Thus, the existing ML approaches stated above can offer high detection accuracy, and industries are eager to find solutions to lower expenses and boost earnings. Maybe a good choice for ML

[6] The most widely used method of payment for online transactions and fraud in everyday purchases is credit cards. Nowadays Fraudsters invent new techniques to commit fraudulent transactions which demand constant innovation for their detection techniques. The majority of methods based on artificial intelligence, fuzzy logic, NN, LR, NB, sequence alignment, DT, Bayesian networks, meta-learning, genetic programming, etc. have been created to identify different types of credit card fraud. Transaction strategies utilized in credit card fraud detection systems are surveyed in this study.

[7] Based on deep learning from a neural network, they employed twelve ML algorithms to detect credit card fraud. They benchmark and real-world performance. In addition to searching the dataset, Ada Boost and majority voting methods are applied to build the hybrid model. The accuracy and sensitivity achieved by the optimal random forest algorithm under the benchmark data are 95% and 91%, respectively. The accuracy rate remains above 90% when tested with real-world data, despite 30% noise in the dataset. MCC (Matthews Correlation Coefficient) is ideal for measuring the performance of a model so the best MCC score is 0.823 and 0.942 for the majority vote adding 30% noise to the dataset.

[8] In this paper, a hybrid technique based on KNN and Naive Bayes is used to detect credit card fraud. The accuracy of KNN is 99.91, whereas the accuracy of naive Bayes is 99.71. KNN will be used as the basic classifier, and it will predict the outcome. The expected outcome will be fed through the Naive Bayes classifier, which will yield the final outcome. The suggested technique is believed to detect credit card fraud with high accuracy.

[9] Researchers are trying to build a model that predicts fraud and non-fraud in credit card transactions using ML algorithms and neural networks. The result of each algorithm is a report for each transaction, with class 0 indicating that the transaction was considered to be valid and 1 indicating that it was determined to be a fraudulent transaction. There are 2,84,807 fraud transactions from Europe cardholders in September 2013, but the data is unbalanced because there are fewer fraud cases than there are transactions. The data set has been converted to a PCA transformation and includes only numeric values. They have a 98.69 percent accuracy rate and scored 94.84 percent for logistic regression, 92.88 percent for decision trees, and 91.62 percent for naive Bayes. The fraud feature has a value of 1 and the normal transaction has a score of 0, and both are classed as non-fraud.

[10] This research uses a dataset of over 30,000,000 separate transactions from a Chinese e-commerce company to analyze fraud and legitimate B2C transactions. Two types of algorithms are used to train the behavior features of legal and illegal transactions. There are 62 attribute values in each record and only around 82,000 transactions were identified as fraudulent in the original dataset. Researchers compare the two random forests, which differ in their basis classifiers, and examine their performance in detecting credit fraud. The capacity of a random forest is determined by two factors: the strength of individual trees and the correlation between them. CART-based random forest was shown to be effective in the first experiment, but the results were worse in the second. Although the precision is slightly lower, the accuracy, recall, and F-measure are much higher. Clearly, the comprehensive performance of the CART-based random forest is considerably superior for usage in this experiment subgroup. Where R stands for the random forest. 0.7811 F-Measure, 91.96% accuracy, 90.27%

precision, 67.89% recall, Random forest based on CART (Random Forest II) 0.9601 F-Measure, 96.77% accuracy, 89.46% precision, 95.27% recall The second experiment is as follows.

[11] The author described a decision tree as a tree-like graph made up of internal nodes that stand in for tests on attributes, branches that indicate the results of the tests, and leaf nodes that represent class labels. The route chosen from the root node to the leaf determines the classification rules. The root node, which is the most obvious property to separate the data, is first selected to divide each input data set. Before the tree is formed, the attributes and values that will be used to analyze the input data at each intermediary node are identified. By moving from a root node to a leaf node and stopping at all internal nodes along the way, the tree can prefigure newly arriving data depending on the test conditions of the characteristics at each node. The primary difficulty lies in deciding which value to use to split a decision tree node.

## III. **Method**

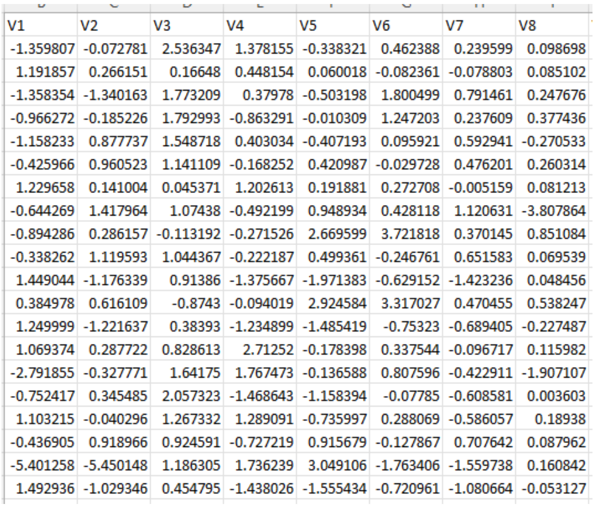
The method proposed in this work utilizes the most recent ML techniques to detect abnormal activities known as outliers. In our datasets, there are 31 columns in this dataset, 28 of which are labeled v1-v28 to safeguard sensitive data. The remaining columns denote Time, Amount, and Class. Time represents the time elapsed between the first and subsequent transactions. Amount refers to the amount of money exchanged. A genuine transaction is represented by class 0, while a fraudulent transaction is represented by class 1. In Figure 1 represents the suggested approach's block diagram, and the specifics are depicted below. We followed the 6 steps for the proposed model. The suggested approach has six major steps: data collection, data processing, choosing a model, training model, model evolution, and prediction.

### 3.1 Data collection

First, we gathered the dataset through Kaggle. Worldline and the ML Group at ULB collected this dataset for analyzing big data mining and fraud detection. This is an up-to-date and standard benchmark dataset in this discipline. This dataset contains 492 frauds out of 284,807 transactions.

### 3.2 Data processing

The dataset contains 492 frauds out of 284,807 transactions that happened over the course of two days. Figure 1 depicts the core dataset in CSV format as well as the sample data visualization.



| V1 | V2 | V3 | V4 | V5 | V6 | V7 | V8 |
|---|---|---|---|---|---|---|---|
| -1.359807 | -0.072781 | 2.536347 | 1.378155 | -0.338321 | 0.462388 | 0.239599 | 0.098698 |
| 1.191857 | 0.266151 | 0.16648 | 0.448154 | 0.060018 | -0.082361 | -0.078803 | 0.085102 |
| -1.358354 | -1.340163 | 1.773209 | 0.37978 | -0.503198 | 1.800499 | 0.791461 | 0.247676 |
| -0.966272 | -0.185226 | 1.792993 | -0.863291 | -0.010309 | 1.247203 | 0.237609 | 0.377436 |
| -1.158233 | 0.877737 | 1.548718 | 0.403034 | -0.407193 | 0.095921 | 0.592941 | -0.270533 |
| -0.425966 | 0.960523 | 1.141109 | -0.168252 | 0.420987 | -0.029728 | 0.476201 | 0.260314 |
| 1.229658 | 0.141004 | 0.045371 | 1.202613 | 0.191881 | 0.272708 | -0.005159 | 0.081213 |
| -0.644269 | 1.417964 | 1.07438 | -0.492199 | 0.948934 | 0.428118 | 1.120631 | -3.807864 |
| -0.894286 | 0.286157 | -0.113192 | -0.271526 | 2.669599 | 3.721818 | 0.370145 | 0.851084 |
| -0.338262 | 1.119593 | 1.044367 | -0.222187 | 0.499361 | -0.246761 | 0.651583 | 0.069539 |
| 1.449044 | -1.176339 | 0.91386 | -1.375667 | -1.971383 | -0.629152 | -1.423236 | 0.048456 |
| 0.384978 | 0.616109 | -0.8743 | -0.094019 | 2.924584 | 3.317027 | 0.470455 | 0.538247 |
| 1.249999 | -1.221637 | 0.38393 | -1.234899 | -1.485419 | -0.75323 | -0.689405 | -0.227487 |
| 1.069374 | 0.287722 | 0.828613 | 2.71252 | -0.178398 | 0.337544 | -0.096717 | 0.115982 |
| -2.791855 | -0.327771 | 1.64175 | 1.767473 | -0.136588 | 0.807596 | -0.422911 | -1.907107 |
| -0.752417 | 0.345485 | 2.057323 | -1.468643 | -1.158394 | -0.07785 | -0.608581 | 0.003603 |
| 1.103215 | -0.040296 | 1.267332 | 1.289091 | -0.735997 | 0.288069 | -0.586057 | 0.18938 |
| -0.436905 | 0.918966 | 0.924591 | -0.727219 | 0.915679 | -0.127867 | 0.707642 | 0.087962 |
| -5.401258 | -5.450148 | 1.186305 | 1.736239 | 3.049106 | -1.763406 | -1.559738 | 0.160842 |
| 1.492936 | -1.029346 | 0.454795 | -1.438026 | -1.555434 | -0.720961 | -1.080664 | -0.053127 |

Figure 1: Sample of the used dataset

The main components derived with PCA are features V1, V2 and V28; those features that have not been altered with PCA are 'Time' and 'Amount.' The 'Time' feature stores the number of seconds that have passed between each transaction and the 1st transaction in the dataset. This dataset is highly unbalanced, that's why datasets need to be pre-processed.

### 3.3 Choosing Model

Model selection is the process of deciding which model will be the one to use as the solution. It is a method that may be used with models of various types as well as with models of the same type but with various model hyper-parameter configurations. The task of picking a statistical model from a group of candidate models given data is known as model selection. The selection of a suitable model is a vital step in putting the ML algorithm into action. More than one algorithm can be used to solve a certain problem. However, the availability of data type, data collection, complexity, resource utilization, and statistical cost function all influence the decision. Regression and classification are two components of supervised ML. In both circumstances, it looks for a certain structure or connection in the input to anticipate the correct output. The dataset determines whether a classification or regression model is used.

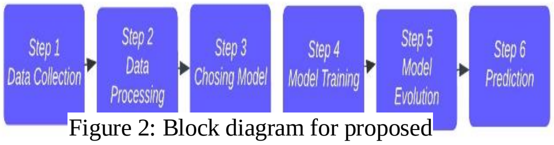


Figure 2: Block diagram for proposed model

When a dataset contains continuous numeric values, regression is required. However, if the dataset contained ins just intended output values, a classifier must be used as the model. The supervised ML classifiers are chosen based on the distinct outcome of this challenge. Model selection is a procedure used by statisticians to analyze the relative value of many statistical models and evaluate which one is the best match for the observed data. As a result, classifier algorithms have been used. The DT, NV, KNN, and RF algorithms have all been used to examine how the data behaves when subjected to various classifiers.

### 3.4 Training model

Model training is fundamental to the advancement of data science. The fundamental phase in ML is model training, which results in a functioning model that can subsequently be verified, tested, and deployed. The performance of the model during training will eventually decide how well it will operate when it is incorporated into an application for end users. The model training phase is focused on the quality of the training data as well as the method selection. Most training data is divided into two sets: training and validation and testing. The model is trained with 284807 data sets and the data shape is (284807, 31). Between the training and testing datasets, there was no interaction**,** hence the test data was unseen to the trained model.

### 3.5 Model Evaluation

We utilize the following equations to evaluate accuracy and precision in our suggested system since those are considered the foundation parameters to evaluate any model. It considers all true and false values, which is why it is often regarded as a balanced measure that can be employed even when there are various classes. Based on equations 1, 2 and 3, accuracy, precision, and recall are calculated respectively.

$$\text{Accuracy} = TP + FP/ (TP + FP + TN + FN) \text{ ……..(1)}$$

$$\text{Precision} = TP / (TP + FP)\text{……………………..... (2)}$$

$$\text{Recall} =TP/TP + FN\text{……………………………… (3)}$$

TP, FP, TN and FN are respectively defined as true positive, false positive, true negative, and false negative.

In Figure 2, the block diagram of the details of the approach are illustrated below. In the diagram proposed seven steps algorithm are shown.

## IV. **Result Discussion**

The experimental outcomes that were discovered during the study are described in this section. The experiment was carried out with the aid of Scikit-learn, a ML tool for Python that is one of the most reliable and practical libraries for ML in the Python language. On our dataset, we tested a few models. There are significant variances in accuracy, precision, and recall among the findings when tabulated. Classification, clustering, regression, and dimensionality are just a few of the capable tools available in Scikit-learn for statistical modeling and ML. This research's solution has led it to select supervised ML classifiers. There are four distinct classifiers used: DT, NV, KNN, and RF. Accuracy, precision, and recall scores are the variables that were taken into consideration during the experiment. Furthermore, K-fold cross-validation (K-CV) is employed to validate the accuracy ratings. K-CV is one of the most extensively used and powerful strategies for testing ML models. Each fold in the K-CV dataset is utilized as a testing set in each iteration, with the dataset being divided into K different folds. The experimental results for recall, cross-validation, and accuracy are reported below in order.

First, Figure 3 displays the accuracy of the suggested systems' performance for each of the selected classifiers. Figure 3 demonstrates that the DT, RF, KNN, and NV accuracy scores are 99.94%, 99.98%, 95.93%, and 99.94%, respectively. The RF classifier has the best accuracy of 99.98%.

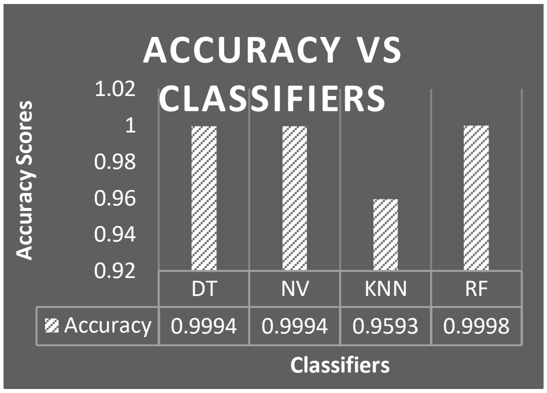


Figure 3: Classifiers vs accuracy

Second, precision scores have been tested to evaluate the performance of the suggested technique. Figure 4 displays the results of all classifiers' precision experiments.

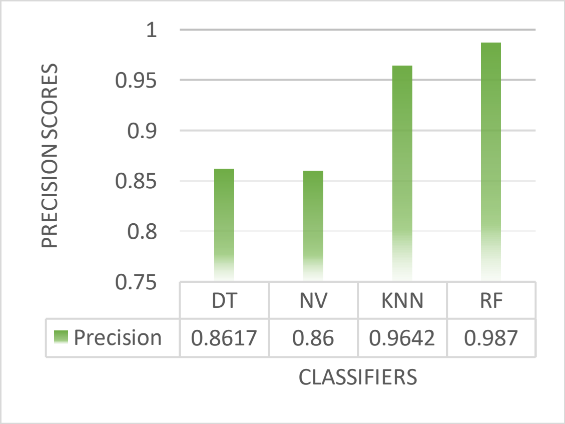


Figure 4: Precision score vs classifiers

The ratio of all positive observations to correctly predicted positive observations is used to determine a precision score. It illustrates how frequently the favorable forecast comes true. The higher the better in this situation. The experiment yielded accuracy scores for DT, RF, KNN, and NV of 86.17%, 98.70%, 96.42%, and 80%, respectively. According to the results, RF produces the best outcomes

.

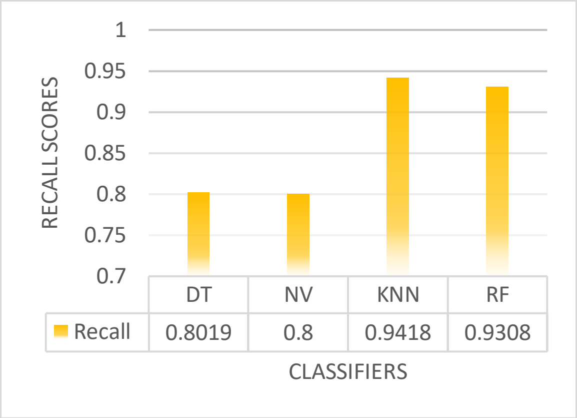


Figure 5: Recall score vs classifiers

The recall score is also used to compute the observation of the true positive prediction number over all of the factual label classes. A recall is also known as sensitivity, and it represents the percentage of true positives. The performance improves as the recall score rises. According to the attained recall score, the corresponding results for DT, RF, KNN, and NV are 80.19%,93.08%, 94.18%, and 80%. But this time, KNN performance received the highest rating (93.08%). The experimental recall scores are displayed in Figure 5.

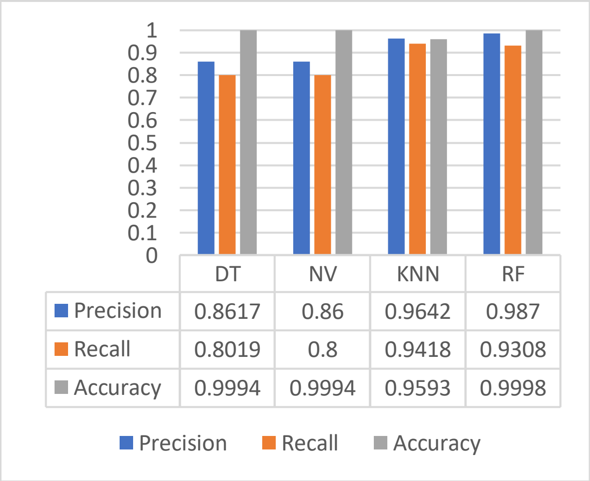


Figure 6: Performance data for all classifiers summarized

Figure 6 illustrates the summary of all the classifiers and shows the accuracy, precision, and recall results for each classifier in a single figure. As can be observed from the image, RF, KNN, and MLP all provide almost identical results, and their score is quite high, in contrast to DT's very low scores.

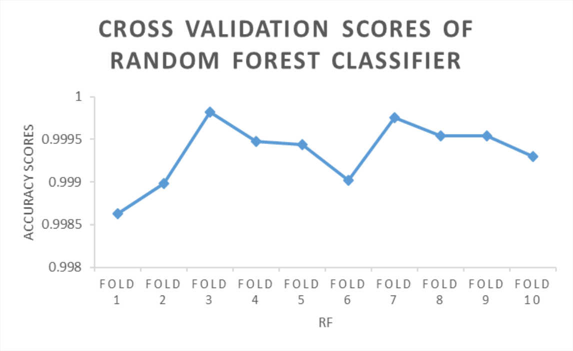


Figure 7: Result KCV for RF classifier

The accuracy of RF is confirmed by the aforementioned figure, which demonstrates that it offers the maximum accuracy. K-CV is performed, and the outcome is shown in Figure 8. The graphic makes it obvious that all K-CV folds produce scores that are quite similar to one another. The fact that there aren't many variances across the folds suggests that the precision is reliable. The test's accuracy being equal, the mean of the 10-fold CV is observed to be 97.04%, validating the RF result. These two K-CV points show that the accuracy determined by the experiment is accurate and that the data used for the experiment is sufficient.

## V. **Conclusion**

In this paper, we have presented an approach to determine whether or not a credit card transaction is fraudulent. We used a complete of 4 category methods Decision Tree, Random Forest, K-nearest neighbors, and Naive Bayes) with an accuracy of 99.94%, 99.98%, 95.93% and 99.94%. Because transaction distributions are not table-bound, credit card fraud occurs frequently, and the perpetrators frequently devise novel ways to carry out their fraudulent activities. Therefore, it will become vital to take into account those converting conduct as nicely at the identical time as growing a predictive version. Hence, an in-depth examination on handling non-table bound nature in credit score card fraud detection might also additionally be performed. However, this has a look at wishes a huge quantity of data.

## **References**

[1]. P. D. C. Soulé-Dupuy, "Credit Card Fraud Detection using," International Journal of Computer Science and Mobile Computing, no. 2022, 2019.

[2]. S. G. Vaishnavi Nath Dornadulaa, "ScienceDirect," Elsevier B.V, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705092030065X. [Accessed 22 October 2022].

[3]. R. R. S. S. D. A. A. P. Nayan Uchhana, "Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 10, no. 6, April 2021, p. 8, 2021.

[4]. M. K. G. Sonal Mehndiratta, "Credit Card Fraud Detection Techniques," International Journal of Computer Science and Mobile Computing, vol. 8, no. 8, p. 7, 2019.

[5]. ai Kiran, J. G., " Credit card fraud detection using KNN,Naive Bayes model-based classifier. *International Journal of Advance Research, Ideas, and Innovations in Technology*, 44-46.

[6]. Chaudhary, R. R. (ISSN: 2278-3075 (Online), Volume-10 Issue-6). A Survey on Credit Card. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*.

[7]. Han, S. (25-26 June 2010,2011). Credit Card Fraud Detection. *2009 International Joint Conference on Artificial Intelligence*.

*[8]*. Darshan kaur(student), c. l. (n.d.). Machine Learning Approach for Credit Card Fraud Detection (KNN & Naïve. *1st international conference on intelligent communication and computational research (ICICCR-2020).*

[9]. V Kumar K S, V.K.V.G., V Shankar A, Pratibha K, Credit card fraud detection using machine learning Algorithms. International Journal of Engineering Research & Technology, 2020

[10]. Xuan, S., et al. Random Forest for credit card fraud detection. in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). 2018. IEEE

[11]. Decision Tree Based Algorithm for Intrusion Detection [Journal] / auth. Kajal Rai M.Syamala Devi,Ajay Guleria. - [s.l.] : Dec 28,2015. - 04 Pages:28282-2834(2016) : Vol. 07.

[12]. SARA MAKKI, Z. A.-S. ( publication July 8, 2019, current version July 29, 2019.). An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. Special Section on Advanced Software and Data Engineering for Secure Societies, 93010.