

## An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods

Naresh Kumar Trivedi<sup>1</sup>, Sarita Simaiya<sup>2</sup>, \*Umesh Kumar Lilhore<sup>3</sup>,  
Sanjeev Kumar Sharma<sup>4</sup>

<sup>1, 2, 3, 4</sup> Chitkara University Institute of Engineering and Technology, Chitkara  
University, Punjab, India

<sup>1</sup>nareshk.trivedi@chitkara.edu.in, <sup>2</sup>sarita.simaiya@chitkara.edu.in,  
<sup>3</sup>umesh.lilhore@chitkara.edu.in, <sup>4</sup>sanjeevk.sharma@chitkara.edu.in

Corresponding author; \*Umesh Kumar Lilhore<sup>3</sup>  
Email: umesh.lilhore@chitkara.edu.in

### Abstract

*With the advent of modern technological advances as well as the modern communications expressways, credit card fraud has been rising substantially. Designed to detect fraud of credit card purchases seems to be a major theme to fundamental economic consequences in financial analysis. Credit card fraud tends to cost millions of dollars per year to consumers and also the financial firm. The fraudsters are continuously seeking out new guidelines as well as strategies to commit illegal activities. Therefore fraud protection technologies have now become important to eliminate the losses of banks and other financial institutions. Throughout this research article, we introduce an effective credit card fraud detection mechanism including a feedback system, dependent on machine learning methodology. Its feedback approach contributes to enhancing the classifier's detection rate as well as cost-effectiveness. Afterward examined the performance of different methodologies incorporates random forest, tree classifiers, artificial neural networks, support vector machine, Naïve Baiyes, logistic regression and gradient boosting classifier strategies, on a slightly skewed credit card fraud data sets. These data sets include transaction data through credit card emerges from European account holders with 284,807 trades. Similar approaches apply towards both raw including and pre-processed content. The efficiency of the approaches has always been evaluated depending on just the performance assessment dimensions for different classifiers, which will include precision, recall, F1-score, accuracy, and FPR percentage.*

**Keywords:** Machine learning methods, Credit Card Fraud Detection, Classification method, Supervised learning.

### 1. Introduction

Now these days digital, statistics are very easily available throughout the world because of digital online availability. All the information that also has a large volume, wide range, frequency, as well as importance is stored from small to large organizations over the cloud. The whole information is available from massive amounts of sources such as followers on social media, customer order behaviors, likes, and shares. White-collar crime is the ever-increasing problem with-reaching consequences for the finance sector, business institutions as well as governments. Fraud can indeed be described as illegal deceit to gain financial benefit [1].

Enhanced card transactions had already appreciated a heavy emphasis on communication technology. When credit card transactions are by far the most prevalent form of transaction for offline and online payments, raising the rate of card fraud accelerates as well.

Machine learning is the innovation of this century that eliminates conventional strategies and also can function on huge datasets where humans can't immediately access. Strategies of machine learning break within two important categories; supervised learning versus unsupervised learning; Tracking of fraud can also be achieved any form and may only be determined how to use as per the datasets. Supervised training includes anomalies to always be identified as before. Many supervised methods are being used over the last few decades to identify credit card fraud. The major obstacle in implementing ML for detecting fraud seems to be the presence of extremely imbalanced databases. Most payments are legitimate in several available evidence sets, with such an extremely small number of fraudulent ones. The significant challenges to investigators are designing the accurate as well as efficient fraud prevention framework that will be low on false positives but efficiently identifies fraud activity [2].

Throughout this study, we introduce an effective credit card fraud identification system with a feedback system, centered on machine learning techniques. That feedback approach contributes to boosting the classifier's detection rate and performance. Also analysis the performance of different classification methods including random forest, tree classifiers, artificial neural networks, supporting vector machine, Naïve Baiyes, logistic regression including gradient boosting classifier approaches, on even a highly skewed credit card fraud database. This complete research paper is divided into different sections including; introduction portion, related activities, credit card fraud obfuscation techniques for machine learning, and the obstacles. Subsequently, the implementation for machine learning techniques as well as the estimation and evaluation of different performance measurement parameters are covered and then the findings of the entire research are covered and also suggested further enhancements.

## 2. Related Work

Machine learning approaches play a crucial role throughout numerous efficient areas for data processing; one of them is the identification of card fraud. Through previous research, several methods were suggested to include strategies for detecting fraud through supervised methods, unsupervised methods including a hybrid strategy; that makes it necessary and know some technology involved in identifying credit card fraud and have a better understanding of the types of card fraud. Many strategies were suggested and checked. Most of them will be reviewed in the brief following.

Detection of card fraud is focused on an interpretation of the card actions in purchases. Most strategies were implemented throughout the identification of card fraud like artificial neural network (ANN), genetic algorithm (GA), support vector machine (SVM), frequent itemset mining (FISM), decision tree (DT), optimization algorithm for migratory birds (MBO) and process for naïve Baiyes (NB). The quantitative logistic regression and naïve bays analysis are conducted in. Bayesian and neural system output is assessed on data concerning credit card fraud [3].

Decision trees, machine learning, and logistical regression are evaluated in fraud detections of the scope. This article [4] evaluates several innovative methods of

machine learning; supporting vector machines including random forests together with logistical regression as part of an attempt towards better detect fraud when applying neural network and logistic regression to identity fraud detection issues. Credit card identification faces many problems because fraud behavioral models are complex. Which are suspicious transactions appear to look like genuine ones; card transaction sets of data are seldom accessible but extremely imbalanced (and skewed); optimum feature choice (parameters) for models; sufficient measures for test the efficiency of distorted credit card fraud database strategies. The efficiency of credit card fraud detecting becomes greatly affected by both the form of sampling approach utilized, parameter choice as well as identification techniques used [5].

There are several different types of credit card fraud. One of these is stealing a physical card while the other is the stealing of confidential credit card information like account number, CVV key, card type, and many others. The fraudster can try to address the significant amount of money and make a massive amount of payment before the cardholder figures out by manipulating credit card information. Now because of this, businesses are using different techniques for machine learning that identify increasing transactions constitute illegitimate and which are not. Whenever a credit card becomes the more common transaction model (respectively online as well as regular transactions), its frequency of fraud tends may accelerate [6].

Designed to detect fraudulent activity utilizing conventional manual methods seems to be time-consuming as well as incorrect, rendering such manual techniques more unrealistic to have the emergence of big data. Financial companies have also transformed into intelligent methods. Such intelligent scam methods comprise methods predicated on computing intelligence (CI). Its techniques for detecting statistical scams are split into two categories: supervised and unsupervised methods. Designs are calculated of supervised techniques in fraud detection predicated on both the specimens in fraud as well as valid exchanges to classify duplicate entries when fraud and valid when statistical anomalies 'exchanges will be identified when prospective cases of fraudulent charges in unsupervised fraud detection[7].

In such a data analysis paper [8] the hybrid data model has been primarily examined by experts when functionality choice, as well as heuristic classification, has been achieved on 3 different levels. Its ordinary preprocessing has been accomplished during the first stage. Four functionality choice algorithms such as genetic algorithm, data gain ratio, as well as an assessment of the recovery characteristics have been used in the second and third phases. Here variables with functionality choice techniques were determined based on both the precision of distinct classification machine learning and then the feature selection technique has been used and this is wisest for a specific classification. Such a hybrid model produced outcomes that were of good precision.

A credit card data collection seems to be strongly imbalanced because it holds more legitimate transfers than that of the fraud. This implies that prediction may acquire a quite high precision rating without identifying the scam transaction. Class allocation, i.e. sampling minority classes, seems to be one great way to deal with such a type of issue. Class learning instances could be doubled even in oversampling significant minority also in reasonable proportion again to the significant majority class so that the new algorithm increases the chance of such correct prediction. Another detailed discussion of such supervised and otherwise unsupervised tools and techniques also can be found at all in this document. There will always fail to detect cases of fraud through supervised optimization techniques. The design in deep autoencoder, as well as restrained Boltzmann machine, is also known as RBM which can build ordinary transfers to discover anomalies from

ordinary trends. It's not only developing the hybrid technique with such a variety of techniques of that same AdaBoost and perhaps Majority Voting [9].

Credit card scam has become too widely known when the digital environment currently has to be. Through staying at home human wants everything within the hand. It tends to increase the use of e-commerce, by which attackers, as well as scammers, have always been compensated for further chance to attempt scam. Its fraudsters usually use many techniques to commit fraud. Recognizing the approach is the requirement to stop more fraud. Something quite a few more previous studies also has been carried out on another variety of techniques to find solutions linked to card fraud identification. All such strategies include, and are not restricted to; neural network models (NN), Bayesian network (BN), intelligent decision engines (IDE), optimization algorithms, meta-learning agents, artificial intelligence, image processing, Constitution-based systems, logic regression (LR), vector support machine (SVM), decision tree, k-nearest neighbor (kNN), meta-learning strategy, adaptive learning, and so on. Its structure of both the neural network becomes primarily used according to an unsupervised technique in using real-time payment processing applications. Self-organizing graph of both the neural network, this can solve this problem from each correlated community using optical classification. With more than just 95 percent of the total detection system of ROC demand curve fraudulent without actually causing any other false alarm ensemble cast learning (also often widely known as meta-classifier) enhances results through combining different learning algorithms optimization algorithms to enhance statistical results [10].

### 3. Machine Learning Methods & Challenges in Credit Card Fraud

Machine learning strategies are often used for the credit scoring framework assessment when they produce fewer presumptions and to provide greater observational precision.

**3.1 Types of Machine Learning Methods:** Machine learning techniques can indeed be separated basically into the categories listed-

#### 3.1.1 Supervised learning

The scheme tries to find out from earlier examples that are provided throughout this learning. So if the set of data has been labeled, under supervised teaching should come. Supervised learning methods have been controlled by initiation, decision trees; scenario-based explanation, supporting vector machines (or SVM), methods of neural networks (NN), linear regression (LR), and neural network used it to detect credit fraud [11];

- **Random Forest:** This is one of the ensemble methodologies used only to improve its prosperity as well as precision in machine learning algorithms of artificial intelligence. One of this kind classifier is the Random Forest (RF), suggested by Breiman, a researcher. A random forest method may also help identify the genuinely appropriate independent variables such that the system may pick functionality. Also, many findings already demonstrate its significance in selecting several possibilities for each shrub, but in empirical research, this is discovered to also be optimal regarding forecast accuracy [12].

- **Naïve Baiyes Classifier:** This is indeed a statistical process based on Predictive theory that selects its greatest probability focused ruling. Unidentified outcomes from recognized value systems have been estimated by Bayesian likelihood. This also enables the implementation of previous knowledge as well as logic in unpredictable assertions. That first methodology seems to have a legally binding independence presumption around characteristics throughout the data.
- **Logistic Regression:** It is another method decided to borrow from either the profession of statistical data by machine learning. It is also the go-to process of issues concerning binary categorization (difficulties with more than just two class moral values). Logistic regression to the mean is used to modeling a class's outcome like actual pass / completely fail, positive and constructive/negative or neutral again and in credit card fraud threat detection cases then we use probability distribution class as fraudulent and not fraud[13].
- **Support Vector Classifier:** A support vector machine-based machine learning method is also known as SVM; mainly a supervised model. This more or less uses classification learning algorithms also for classification major problems even in two groups and individuals. They really can classify a new document since giving the number of the labeled dataset to each classification on an SVM system.
- **K-Nearest Neighbors (kNN):** A K-nearest Neighbors (KNN) classifier seems to be a straightforward, simple-to-implement supervised machine learning algorithm that could be used to address respectively classification as well as regression difficulties.
- **Classification Trees:** The Classification tree marks, records, as well as allocates separate class factors. The Classification tree may provide a charisma measure that perhaps the category becomes accurate. The Classification Tree has been constructed via a process called binary recursive partitioning [14].
- **Artificial Neural Networks:** This is a kind of machine learning method patterned on the brain and nervous system. Utilizing historical information, its ANN designs may discover the trends, and also can classify the incoming data.
- **Gradient Boosting (GBM):** Gradient Boosting is also known as the GB method, is a prominent algorithm of machine learning, always had to conduct classification as well as regression activities. The above model consists of such an amount in fundamental ensemble designs such as feeble decision trees. Such decision trees combine to create a powerful specular reflection-boosting model [15].

### 3.1.2 Unsupervised learning

Unsupervised training seems to be a class of techniques of Machine learning to discover trends of records. The techniques will be abandoned to themselves in unsupervised learning, to discover fascinating constructions inside the data. K-means method, Self-organizing Map method also known as SOM, as well as the Hidden Markov Model method (HMM), are the most popular unsupervised techniques [16].

### 3.2 Challenges in Credit Card Fraud Detection

The challenge would be to acknowledge fraudulent transactions such that merchant accounts 'customers are not charged for transactions that they didn't perform [17]. The

infield of credit card fraud detection several challenges still needs to address. Some of them we are covering here.

**Major challenges of identifying credit card fraud seem to be:**

- **Enormous information** has been stored on even a daily basis as well as the design construction should be quick enough yet to react properly to a fraud.
- **Imbalanced information**, i.e. its majority of transactions (98.9%) is also not fraud, making it impossible to identify fraudulent activity.
- **Misclassified information** might be another major issue because not all fraudulent activity is captured or recorded.
- **Adaptive methods** used among fraudsters against the system.

## **4. Implementation & Result Analysis**

Author Throughout this research paper, we portray an efficient credit card fraud detection system with such as feedback framework, predicated on machine learning techniques. Its feedback technique contributes to enhancing its classifier's detection rate as well as efficiency. Afterward analyzed its performance of formerly different methods includes random forest method, tree classifiers method, artificial neural networks method, supporting vector machine method, Naïve Baiyes method, logistic regression method and gradient boosting classifier methods, on even a skewed credit card fraud dataset. For the implementation of the machine learning method for credit card data set, we have collected data from European cardholder which mainly contains transactions data through credit card emerges with total 284,807 transactions. Such methods extend to both raw as well as pre-processed information. Performance of both the methods has been evaluated based on both the performance measurement variables of different algorithms, which include precision, recall, F1-score, accuracy as well as FPR percentage.

### **4.1. Credit Card Database**

A set of data seems to be from the ULB Machine Learning Community, as well as the explanation could be discovered on both the website of Kaggle. That dataset includes transactions by European credit cardholders throughout the year 2013. The whole dataset introduces transactions that occurred of two days, composed for 284,807 transactions, the number of 492 transactions being such a fraud. The whole data sets seem to be strongly unbalanced so this set of data may have features applicable mostly to V1 ..... V28; Principal Component Analysis, etc and time, class and quantity are also non-PCA based primarily features. Class is already completely broken down into two subcategories 0 and as well as 1. Where all the class 1 is a fraud, and perhaps 0 is non-fraud data collected [18].

### **4.2 Steps in Credit card Fraud Detection**

Figure 1.1 shows the different steps used during identifying credit card (CC) fraud utilizing machine learning techniques. This is followed by steps-

- 1) Start gathering data available and upload the credit card set of data.
- 2) Use one-class classifiers as well as the Matthews correlation coefficient to extend data pre-processing as well as confirm multiple imbalances throughout the data.
- 3) Plot Dataset Correlation Matrix for the whole dataset.

- 4) Split the data into the subgroups in training and testing, e.g. 70 percent as training as well as 30% also as testing.
- 5) Utilize classification system (Machine Learning) methodology.
- 6) Calculate the total the different metrics of the evaluation, including confusion matrix (Table 1.1), accuracy, precision, recall (or TPR), f1-score, FPR using equations-

$$\text{Precision} = (\text{True Positive} / \text{True Positive} + \text{False Positive}) \text{-----}(1)$$

$$\text{Recall} = (\text{True Positive} / \text{True Positive} + \text{False Negative}) \text{-----}(2)$$

$$\text{F1 Score} = \{2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) \text{-----}(3)$$

$$\text{Accuracy} = \{(\text{True Positive} + \text{True Negative}) / (\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative})\} \text{-----}(4)$$

$$\text{Recall or True Positive Rate} = \{(\text{True Positive}) / (\text{True Positive} + \text{False Negative})\} \text{-----}(5)$$

$$\text{False Positive Rate} = \{(\text{False Positive}) / (\text{False Positive} + \text{True Negative})\} \text{-----}(6)$$

		Actual Value	
		Positive (1)	Negative (0)
Predicted Value	Positive (1)	TP	FP
	Negative (0)	FN	TN

Table 1.1 Confusion Matrix

- 7) Apply feedback method to improve the detections rate and accuracy.
- 8) Repeat steps from step from 4 to 6 for various classifiers.

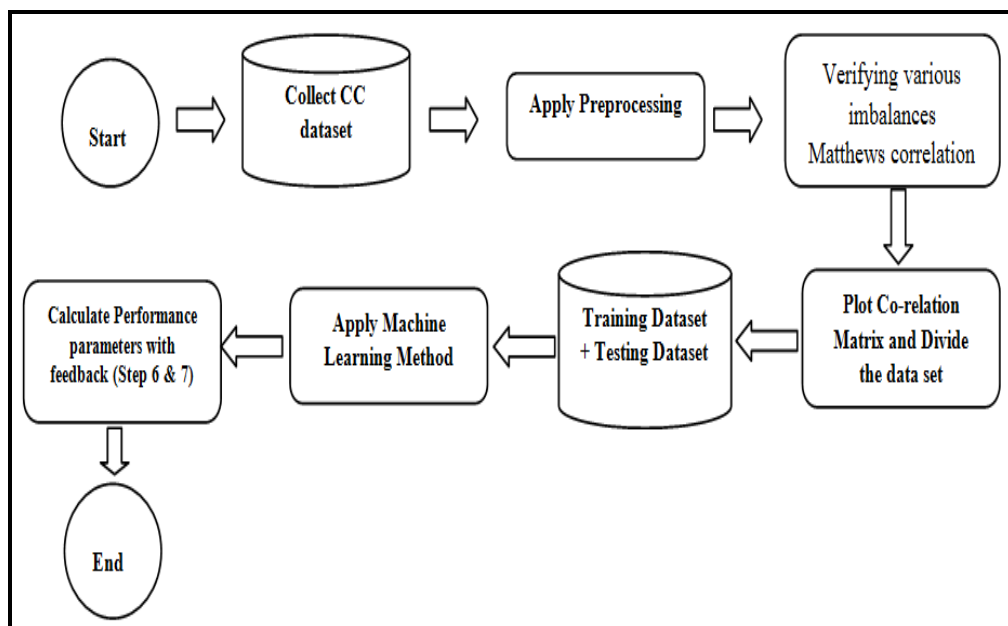


Figure 1.1 Steps in CC Fraud Detection Using ML

#### 4.3 Experimental Results:

Various parameters for measuring performance have been computed. In this data analysis python programming language is being used to implement different classifier algorithms of machine learning to confirm credit card fraud from those in the dataset. During implementation, the data set has been divided into two categories of 70 % for training and 30 % for testing.

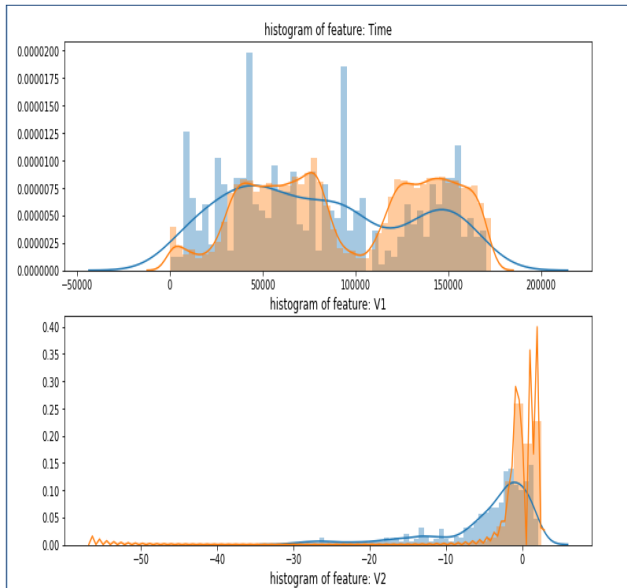


Figure 1.2 Histogram for feature Time feature from V1 to V28

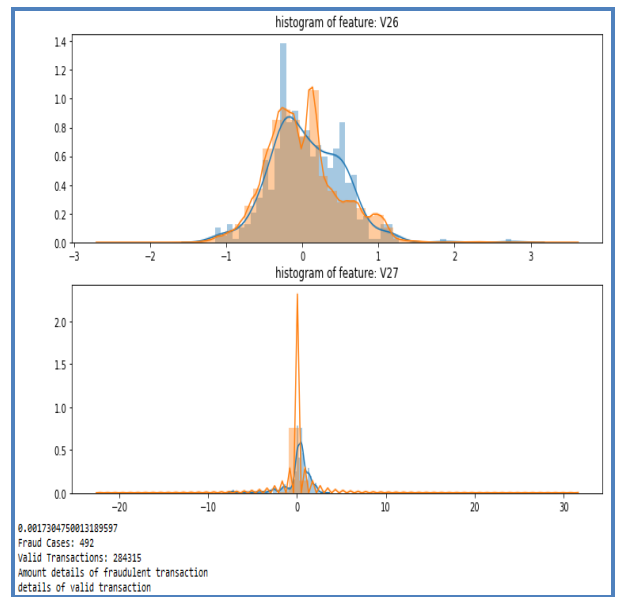


Figure 1.3 Histogram for the

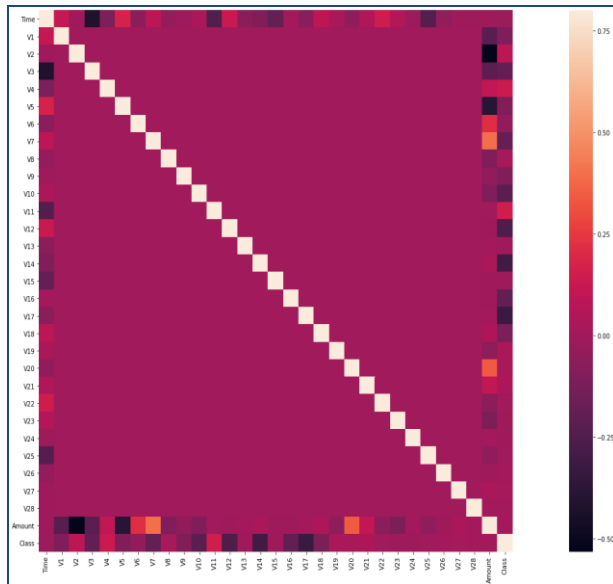


Figure 1.4 Co-relation Matrix for CC dataset Dataset

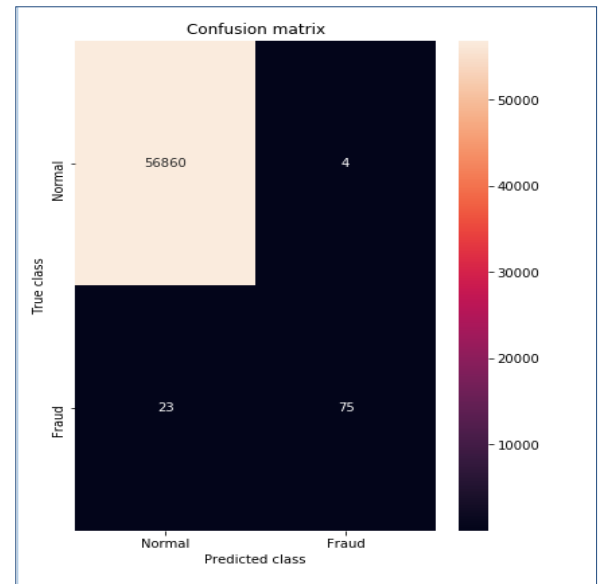


Figure 1.5 Confusion Matrix for CC

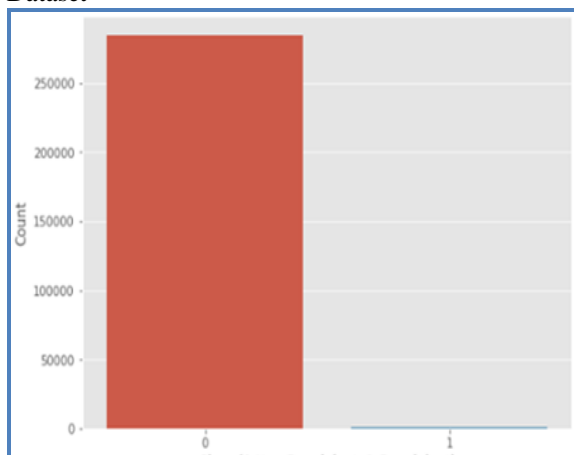


Figure 1.6 Class 0 Frauds & 1-Nonfraud

Based on experiments various parameters have been calculated for CC dataset. Figure 1.2 shows the histogram for feature time and other features e.g V1 to V28. Figure 1.4 is showing co-relation matrix, figure 1.5 shows confusion matrix and figure 1.6 shows class result (Class 0 for fraud and Class-1 Non fraud) for credit card data set. Accuracy, sensitivity, specificity, precision are used to evaluate the performance of the four classifiers. The true positive, true negative, false positive and false negative rates of the classifiers in each set of un-sampled are shown below in Table 1.2. Performance of classifiers varies across different evaluation metrics.



Evaluation Parameters in %	Machine Learning Classifiers						
	Random Forest	Naïve Baiyes	Logistic Regression	SVM	kNN	Decision Trees	GBM
Precision	95.9887	91.201	92.8956	93.228	94.5891	90.998	93.998
Recall	95.1234	91.989	93.112	93.005	92.008	91.996	93.001
F1-Score	95.1102	91.7748	92.112	93.479	91.003	92.778	93.998
Accuracy	94.9991	91.8887	90.448	93.963	94.999	90.998	94.001
Recall	95.1023	91.0021	91.5456	92.789	91.998	91.7752	93.556
FPR	3.9875	4.7789	3.9785	3.889	3.998	4.665	4.665

Table 1.2 Experimental Results for Various ML Methods

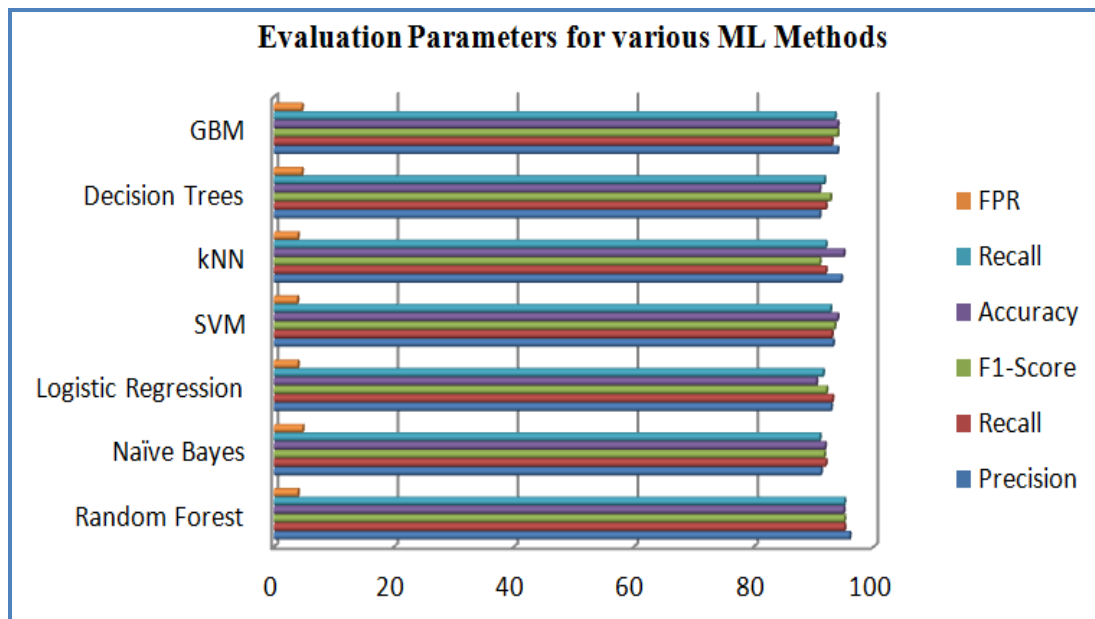


Figure 1.6 Experimental Results for Various ML Methods

Experimental results from Table 1.2 as well as Figure 1.6 demonstrate the percent of the different assessment parameters for just the credit card fraud dataset for distinct machine learning techniques. Findings indicate that random forest techniques demonstrate an accuracy percentage with 95.988 percent, although SVM 93.228 percent, LR 92.89 percent, NB 91.2 percent, Decision trees 90.9 percent as well as GBM 93.99 percent demonstrate a precision percentage of ULB machine learning credit card fraud identification. For any machine learning technique, greater values are shown to be accepted as just a higher performance method of precision, accuracy, recall, and F1-score. As we have seen, there are a few algorithms that have surpassed others as well quite significantly. Thus, selecting Random Forest over all other techniques (Figure 1.6) could be a sensible approach in attaining a greater degree of completeness when decreasing quality just significantly.

## 5. Conclusions & Future Works

Credit card fraud has without hesitation an expression of criminal deception. Fraud identification seems to be a complicated problem that requires a significant amount of skill until throwing algorithms regarding machine learning into it. However, it is an implementation for both the better of machine learning as well as

artificial intelligence, ensuring that perhaps the funds of both the customer seems to be secure and therefore not manipulated. The whole research article addressed an effective system of identifying fraud depending on machine learning methodologies, with such a feedback system. Its feedback process relates to enhancing the classifier's detection rate as well as effectiveness. An observational analysis has been conducted on respective machine learning strategies except for random forest, tree classifiers, artificial neural networks, vector supporting machine, Naïve Baiyes, logistic regression as well as gradient boosting classifier techniques, but also multiple performances evaluating parameters have been calculated such as precision, recall, F1-score, accuracy, and FPR percentage, for any method which has better results for evaluation parameters can be treated as best performing method. Here Random forest is showing better results as compared to other machine learning classifiers.

In future work proposed method can be implemented and tested on large size real-time data with different more machine learning methods.

## References

- [1] Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017, October. Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNi) (pp. 1-9). IEEE.
- [2] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of System Assurance Engineering and Management*, 8(2), pp.937-953
- [3] Fu, K., Cheng, D., Tu, Y. and Zhang, L., 2016, October. Credit card fraud detection using convolutional neural networks. In *International Conference on Neural Information Processing* (pp. 483-490). Springer, Cham.
- [4] Yee, O.S., Sagadevan, S. and Malim, N.H.A.H., 2018. Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 10(1-4), pp.23-27.
- [5] Khan, A.U.S., Akhtar, N. and Qureshi, M.N., 2014. Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm. In *Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing, ITC* (pp. 113-121).
- [6] Carneiro, N., Figueira, G. and Costa, M., 2017. A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems*, 95, pp.91-101.
- [7] Dhankhad, S., Mohammed, E. and Far, B., 2018, July. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In 2018 IEEE International Conference on Information Reuse and Integration (IRI) (pp. 122-125). IEEE.
- [8] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of System Assurance Engineering and Management*, 8(2), pp.937-953.
- [9] Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F., 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences*, 479, pp.448-455.
- [10] Bahnsen, A.C., Stojanovic, A., Aouada, D., and Ottersten, B., 2014, April. Improving credit card fraud detection with calibrated probabilities. In *Proceedings of the 2014 SIAM international conference on data mining* (pp. 677-685). Society for Industrial and Applied Mathematics.
- [11] Popat, R.R. and Chaudhary, J., 2018, May. A survey on credit card fraud detection using machine learning. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1120-1125). IEEE.
- [12] Patil, S., Nemade, V. and Soni, P.K., 2018. Predictive modelling for credit card fraud detection using data analytics. *Procedia computer science*, 132, pp.385-395.

- [13] Malini, N. and Pushpa, M., 2017, February. Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication, and Bio-Informatics (AEEICB) (pp. 255-258). IEEE.
- [14] Zareapoor, M. and Shamsolmoali, P., 2015. Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), pp.679-685.
- [15] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2015, July. Credit card fraud detection and concept-drift adaptation with delayed supervised information. In 2015 international joint conference on Neural networks (IJCNN) (pp. 1-8). IEEE.
- [16] Mahmoudi, N. and Duman, E., 2015. Detecting credit card fraud by modified Fisher discriminant analysis. Expert Systems with Applications, 42(5), pp.2510-2516.
- [17] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.E., He-Guelton, L. and Caelen, O., 2018. Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, pp.234-245.
- [18] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), pp.3784-3797.

## Authors Profile



**Dr. Naresh Kumar Trivedi** is a Professor in CSE at Chitkara University, Punjab. He has experience of 26 years in Teaching, Research and industry. He has Published 14 research Paper and 4 Patent. He has a strong academic background in Computer Science. His research major research areas include Data Mining, Machine Learning.



**Dr. Umesh Kumar Lilhore** is an Associate Professor at Chitkara University Institute of Engineering and Technology, Punjab, India. He received his PhD & M Tech in Computer Science Engineering. He has more than 13 years of experience in education, research and consultancy. He has published more than 50 research articles in leading journals, conference proceedings and books of high repute. His research interests mainly includes Artificial Intelligence, Machine learning, IoT, Computer Security, Computational Intelligence and Information Science.



**Dr. Sarita Simaiya**, is an Associate Professor at Chitkara University Institute of Engineering and Technology, Punjab, India. She received her PhD, M Tech & BE in Computer Science Engineering. She has published more than 20 research articles in leading journals, conference proceedings and books of high repute. Her research area includes Wireless Sensor Network, Artificial Intelligence, Machine learning and Security.



**Dr. Sanjeev Kumar Sharma** is working as a Professor at Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. He is PhD in Computer Science and M. Tech in Computer Science & Engineering. He has research publications in International journals of high repute. He has also published 23 books and 5 patents till date. His research area includes AI, Machine learning, Design and Analysis of algorithms, and Networking.