Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Credit Card Fraud Detection Using Machine Learning Algorithms Using Python Technology

Neha Purohit and Dr. Rajeev G. Vishwakarma

Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam University, Indore (M.P.) 452010, India

Corresponding Author Neha Purohit

Abstract— Banking and finance are the backbones of any country's economy. Financial frauds are the most crucial which impact the banking sector as well as the economy. Therefore credit card fraud detection is one of the essential parts of the banking system. However there are various manual and machine learning-based solutions available for detecting and preventing potential frauds, but most of the techniques are not accurate to provide reliable predictions about fraud cases. Therefore the proposed work is aimed to design and develop a machine learning model for preventing financial fraud more specifically for credit card fraud. In this context first, a machine learning model has been introduced and then using different machine learning algorithms the potential of a fraud detection system has been measured. In this experiment, we involved k-means clustering, random forest, k-nearest neighbor (k-NN), Naïve Bays classifier, Logistic regression, Convolutional neural network, and support vector machine. The experimental analysis of the proposed model has been carried out based on a publically available dataset based on Kaggle. However, the dataset has significantly higher dimensions thus correlation coefficient has been used for selecting effective features from the given dataset. The implementation of these models has been carried out using python technology. The experimental performance of the proposed system indicates that the supervised learning processes are more accurate than the unsupervised learning models. According to the experimental analysis, we have found the models SVM, CNN, RF, and LR are providing higher accuracy as compared to k-means, KNN, and GNB. Additionally, the performance in terms of training time LR and CNN is more efficient than the SVM and RF. Thus according to the overall performance, we have selected CNN and LR for extension of the described work in this paper.

Keywords—Machine Learning, Classification, Credit card fraud detection, machine learning application, supervised and unsupervised learning, comparison.

I. INTRODUCTION

India is a raising country due to which a number of new changes are rapidly occurring in our daily life. One of the great changes is the method of payment which is frequently moved from cash to various digital payments medium [1]. Among different payment channels, the credit card is one of the most popular mediums of payment processing. However, banking companies are aware of

digital fraud but there are various innocent credit card users who are not much aware of digital fraud [2]. In this context, we need a security technique, which is able to capture the patterns of credit card usage and estimate the possible fraud cases [3]. In order to deal with this issue, a number of contributions are already available based on machine learning techniques. But which machine learning technique will perform most accurately is need to be known. Therefore in this presented work, we proposed to conduct a comparative performance study among different machine learning algorithms has been carried out.

The study is motivated by some recent contributions, according to V. B. Nipane [4] with growing advancements in e-commerce, fraud is spreading all over the world, causing major financial losses. Decision trees, Genetic algorithms, Meta-learning strategy, neural networks, and HMM are the presented methods used to detect credit card frauds. In contemplating a system for fraudulent detection, the artificial intelligence concept of Support Vector Machine (SVM) & decision tree is used. By implementing this approach, financial losses can be reduced to a greater extent. Similarly, according to K. Gowthami et al [5] credit card fraud results from misuse of the system and is defined as theft or misuse of one's credit card information without the permission of the cardholder. To detect such frauds, it is important to check the usage patterns of a user over past transactions. Credit card fraud refers to the physical loss of a credit card or loss of sensitive credit card information. Many machine learning algorithms can be used for detection.

Next, S. Kiran et al [6] present the Naïve Bayes improved K-Nearest Neighbor method (NBKNN) for Fraud Detection of Credit Card. Results illustrate that both classifiers work differently for the same dataset. The purpose is to enhance the accuracy and enhance flexibility of the algorithm. According to C. Sudha et al [7], the KNN algorithm is an evolutionary search and optimization technique that Mimics natural evolution to find the best solution. Here the characteristics of credit card transactions undergo evolution to allow a modeled credit card fraud detection system. This method proves accurate in deducting fraudulent transactions and minimizing the number of false alerts. If this algorithm is applied to a bank credit card fraud detection system, the probability of fraudulent transactions can be predicted soon after credit card transactions. D. Meenakshi. B et al [8] focussed on credit card fraud detection in the real world. Implementation of fraud detection systems has become imperative for all credit card issuing banks to minimize losses. One of the most crucial challenges is that neither the card nor the cardholder needs to be present when the purchase is being made. This makes it impossible for the merchant to verify whether the customer making a purchase is authentic or not. With the given scheme, using a random forest algorithm the accuracy of detecting fraud can be improved. The random forest is used to analyze the data set. Finally, optimize the accuracy of the result data. The performance is evaluated based on accuracy, sensitivity, specificity, and precision.

Fraud detection based on the analysis of existing purchase data of cardholders is a promising way to reduce the rate of successful credit card fraud. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system. D. Viji et al [9] model the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and K-means clustering. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM, it is considered to be

fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. Similarly, Y. Abakarim et al [10] focus on one of the systems for fraud detection to have a more accurate and precise. Therefore, many solutions and algorithms using machine learning have been proposed in the literature. However, comparison studies exploring Deep learning paradigms are scarce, and to our knowledge, the proposed works don't consider the importance of a Real-time approach. Thus, to cope with this problem authors [10] propose a live credit card fraud detection system based on deep neural network technology. The model is based on an auto-encoder and permits to classification, in real-time, of credit card transactions as legitimate or fraudulent. The Benchmark shows more promising results for our proposed model than existing solutions in terms of accuracy, recall, and precision.

Machine learning algorithms have different techniques and methods to analyze the data. Thus the classification performance of the different algorithms has varied accordingly [11]. Therefore, in this paper first, we provide a quick overview of different machine learning algorithms which are utilized in previous research works. In the next step, we have designed a model for credit card fraud detection. Additionally, we have trained seven different machine learning algorithms. Based on the experimental analysis of a publically available dataset the performance of the proposed model has been evaluated. Finally based on experimental evaluation the conclusion and future extension of the presented study have been highlighted.

II. RESEARCH BACKGROUND

This section involves the study of different machine learning algorithms, which are being used in the proposed credit card fraud detection system.

1) SVM (Support Vector Machine):

SVM is one of the most popular ML techniques for data classification. It can be used to classify linear as well as nonlinear data. The goal is to separate the two classes using a function prepared using training data [12]. The SVM is maximizing the margin during classification. It is used to solve binary classification problems. The classifier is finding the hyper-plane with the largest margin; training data are not always linearly separable [13]. Thus to handle the nonlinearly some slack variables have been used to tolerate training errors. This variable is referred to as a soft margin. The SVM classifier creates one or multiple hyperplanes for classification and regression. For the two-dimensional linearly separable data, we can separate the data by a line. The function of the line is:

$$y = ax + b \dots\dots\dots\dots\dots\dots (1)$$

If we rename x with x_1 and y with x_2 then the line equation can be defined as:

$$ax_1 - x_2 + b = 0 \dots\dots\dots\dots\dots\dots (2)$$

Now, if we define $x = (x_1, x_2)$ and $w = (a, -1)$, then:

$$w \cdot x + b = 0 \dots\dots\dots\dots\dots\dots\dots (3)$$

This is the equation of the hyperplane. Once we have the hyperplane, we can then use the hyperplane to make predictions. We define the hypothesis function h as:

$$h(x_i) = \begin{cases} +1 & \text{if } w \cdot x + b \geq 0 \\ -1 & \text{if } w \cdot x + b \leq 0 \end{cases} \dots\dots\dots\dots\dots\dots (4)$$

The hyperplane will be classified as class +1, and the point below the hyperplane will be classified as class -1.

2) Logistic Regression

Logistic Regression was basically used in the biological sciences. It was then used in many other applications. It is used when the target variable is categorical [14] [15]. For example, in a classification problem, this results in true or false. Such as in a classification problem we need to classify an input X into positive or negative. So, in a Simple Logistic Regression Model

Output = 0 or 1

Hypothesis = $Z = WX + B$

Where, W is the weight and B is a constant

$h\Theta(x) = \text{sigmoid}(Z)$

$$\text{sigmoid}(Z) = \frac{1}{1 + e^{-z}} \dots\dots\dots (5)$$

If 'Z' goes to infinity, Y will become 1 and if 'Z' goes to negative infinity, Y will become 0.

3) Gaussian Naïve Bayes

The Naive Bayes classification is a probabilistic classifier. This can derive by using Bayes' theorem. Based on nature, we train the Naive Bayes algorithm as supervised learning. There are two types of probabilities are used [16]:

- Posterior Probability

[P (H/X)]

- Prior Probability

[P (H)]

Where, X is data and H is assumption. Thus Baye's Theorem stated as:

$$P\left(\frac{H}{X}\right) = \frac{P\left(\frac{X}{H}\right) P(H)}{P(X)} \dots\dots\dots (6)$$

4) K-Nearest Neighbor Classification

The KNN is a lazy learning classifier and classically utilized for both prediction and classification tasks. The KNN algorithm is working in three main steps first the algorithm finds the distance between the queried sample and all the training samples [17]. In order to measure the distances mostly Euclidean distance will be used. Euclidean is described by:

$$d(p, q) = \sqrt{\sum_{i=1}^{N} (q_i - p_i)^2} \dots\dots\dots\dots\dots (7)$$

Where q is the query vector and p is the dataset samples.

After calculating the distance among both the samples the algorithm assigns a class label to the queried sample. The class label is assigned based on the k nearest samples from the training sample. Here the k will be an integer, which is provided by the designer. The k-NN is not required a large amount of data for learning. It is the major advantage of the algorithm [18].

5) Random Forest

Random forests are an ensemble learning technique for classification and regression. That is constructed by a number of decision trees during training. During classification, the output of the random forest is calculated by most tree outputs [19]. The random forest can also be used for regression or prediction tasks. In order to predict a continuous value using the random forest, the mean prediction of all the developed trees is used. The Random forest develops multiple trees by which it overcomes the issues of overfitting which is very common in individual decision tree algorithms. Random forests are normally more accurate than individual decision trees, but their accuracy is lower than gradient-boosted trees [20].

6) K Means Algorithm

The k-means clustering is an unsupervised learning algorithm. The k-means algorithm can directly work on the input dataset for creating groups of similar behavior data. The algorithm first accepts the number of clusters to e created. The algorithm selects k random samples from the dataset which is called the centroid. In the next step, the algorithm finds the distance between the centroids and all the training samples. The distance can be defined as:

$$d(x,y) = \sqrt{\sum_{i=1}^{N} (x_i - y_i)^2} \dots\dots\dots\dots\dots\dots (8)$$

In the third step based on the distance, the training samples are assigned to the centroids. Further, the selected centroids are updated by using the mean of all the samples which are assigned to a centroid. This process is performed in an iterative manner till the objective is not converged [21].

7) Convolutional neural network

The Convolutional neural network (CNN) is an advanced form of artificial neural network. That is basically prepared for the classification and recognition of image data objects. But this technique is now being used in various other classification and regression tasks. The CNN can consist of various layers such as the input layer, max pooling layer, and normalization layers for extracting features from the data samples. Then the backpropagation or dense layers are used for training with the extracted features from the data samples [22].

This section provides a brief overview of the different machine learning algorithms which will be used for credit card fraud detection. The next section provides a detailed overview of the proposed model for credit card fraud detection.

III. PROPOSED WORK

The proposed model for credit card fraud detection is described in Fig. 1. The model consists of the different functional components which are used for processing the input data samples and predicting potential credit card frauds.

Input Training samples: It is important to recognize fraudulent credit card transactions by credit card issuing companies so that customers are not charged for items that they did not purchase. This dataset contains credit card transactions made in September 2013 by European cardholders. The dataset has 492 frauds out of 284,807 transactions. The dataset is highly unbalanced. It

contains only numerical input variables which are the result of a PCA, due to confidentiality issues it cannot provide the original features. The only features which have not been transformed are 'Time' and 'Amount'. Feature 'Class' is the response variable and it takes a value of 1 for fraud and 0 otherwise.

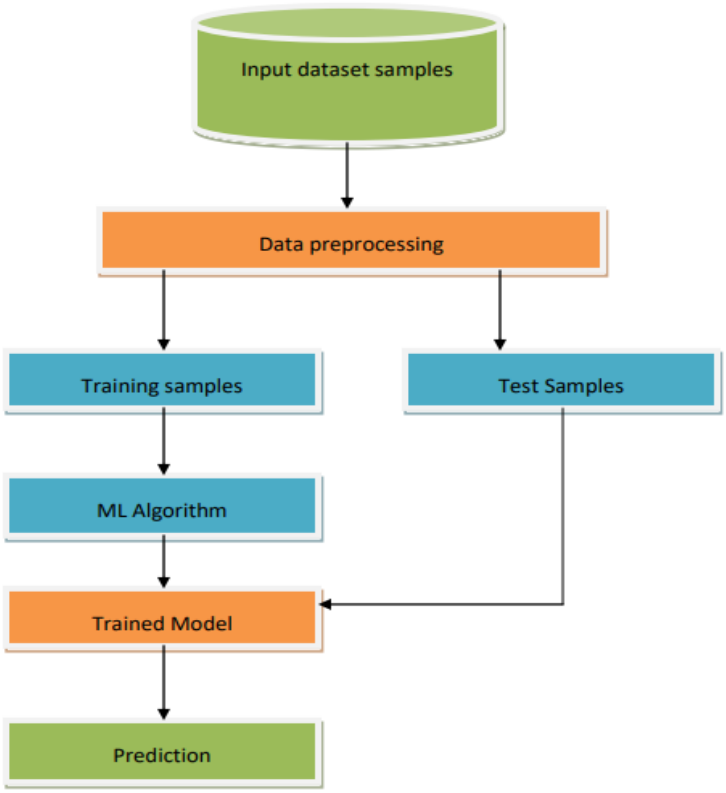
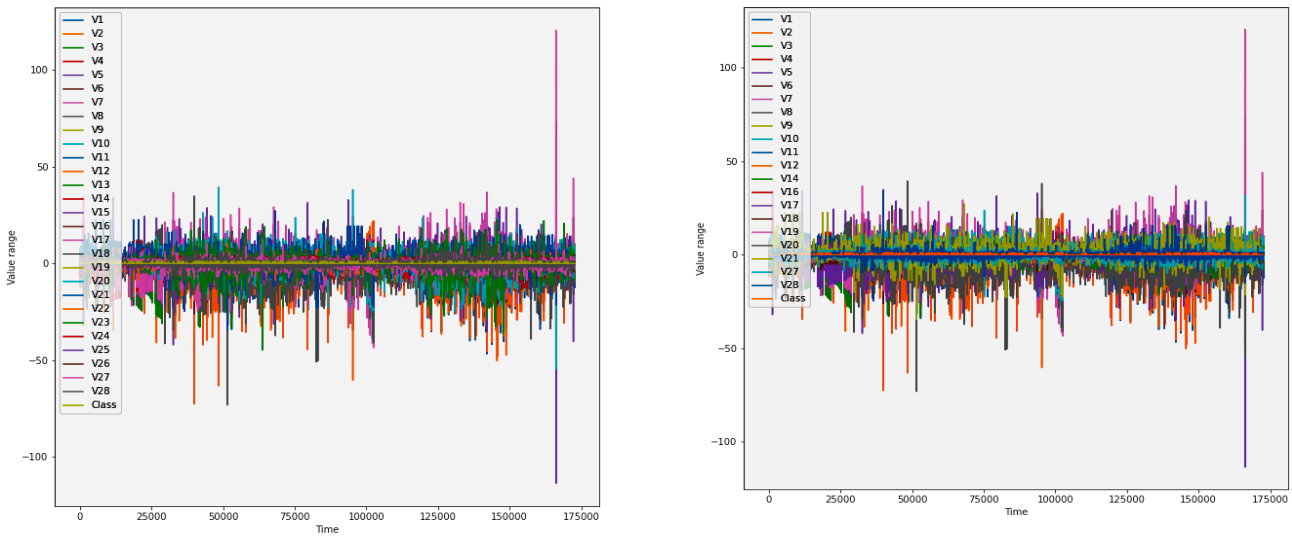


Figure 1: Proposed model

Data pre-processing: Data pre-processing is an essential part of machine learning-based problem-solving techniques. In this context, different techniques are applied to clean and transform the data.

In this presented work first, we visualized the data for understanding the pattern of information obtained from the dataset. Fig. 2(A) demonstrates the initial plot of the entire data samples. Additionally, after data pre-processing the data is visualized in figure 2(B).



(A) (B)

Figure 2: Demonstrate the data samples (A) before data pre-processing and (B) after data pre-processing

In order to pre-process the dataset, we have used the correlation coefficients among the dataset features and the class labels of the dataset. The correlation coefficient can be described by the following equation:

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}} \dots\dots\dots\dots (9)$$

Where, x_i and y_i is the values of the samples, $\bar{x}$ and $\bar{y}$ are the mean of the samples.

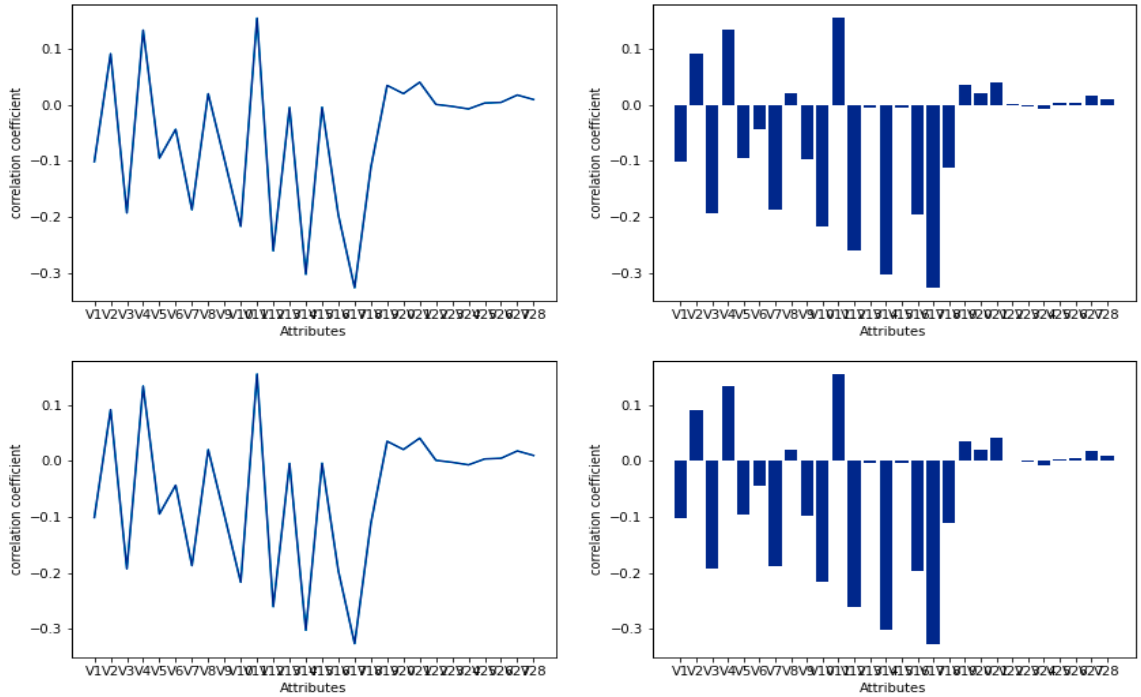


Figure 3: Correlation coefficient for dataset attributes

The estimated correlation coefficient of the attributes with respect to their class labels are demonstrated in Fig. 3. In this figure the line graph as well as their bar graph representation is

demonstrated. The values of correlation coefficient will be used to identify the more essential attributes as compared to less meaningful attributes. After data pre-processing the data samples contain only 22 attributes and one class label. This dataset is next split into two parts i.e. training and testing. The training set contains 75% of the entire data samples and 25% of samples are used for validation or testing of the model. Finally, the training samples are used to train the selected ML models which are described in section II. The training of the models has results in the trained model which is used for classifying the validation set. The classification consequences are described in the next section.

IV. RESULTS & DISCUSSION

The proposed work basically aimed to design a credit card fraud detection model using machine learning algorithms. Therefore we need an efficient and accurate ML model for this task. In this context, in this paper, we proposed to compare different machine learning algorithms which are recently been used in different credit card fraud detection models. The proposed comparative study involves the seven machine learning algorithms namely Logistic Regression (LR), Random Forest (RF), K nearest Neighbors (KNN), Gaussian naive Bayes (GNB), Support vector machine (SVM), K-means, and Convolutional neural network (CNN). The performance of the models is measured in terms of precision, recall, f-score, and accuracy.

Table 1: Performance of the ML classifiers for classifying the credit card fraud detection model

Algorithms →	LR		RF		KNN		GNB		SVM		K-means		CNN	
Classes →	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Precision	1.00	0.87	1.00	0.95	1.00	0.07	1.00	0.07	1.00	0.85	1.00	0.01	1.00	0.79
Recall	1.00	0.57	1.00	0.79	0.98	0.83	0.98	0.83	1.00	0.76	0.98	0.07	1.00	0.81
F1-score	1.00	0.69	1.00	0.86	0.99	0.13	0.99	0.13	1.00	0.80	0.99	0.01	1.00	0.80
Accuracy	1.00		1.00		0.98		0.98		1.00		0.98		1.00	

Precision is also known as positive predictive value. That is the fraction of relevant instances among the retrieved instances. Precision is defined as follows:

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \dots\dots\dots (10)$$

Where, TP indicates the True Positive, and FP shows the False Positive ratio.

Recall is also known as sensitivity or true positive rate and is defined as follows:

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \dots\dots\dots (11)$$

Where, FN shows the False Negative ratio.

F1-score is a metric which takes into account both precision and recall therefore that is a harmonic mean of precision and recall in order to describe the quality of classification outcomes. It is defined as:

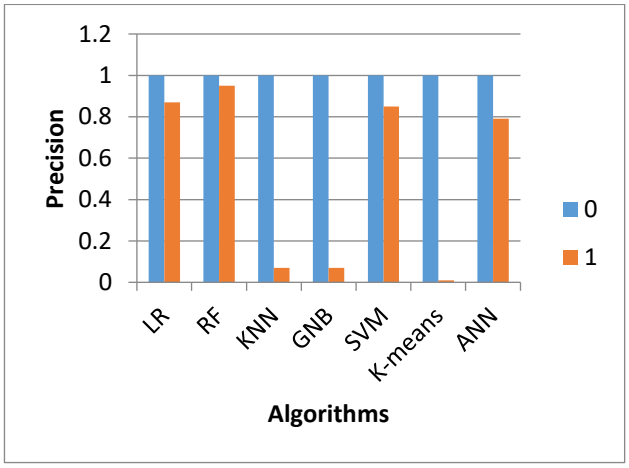
$$\text{F1} - \text{Score} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \dots\dots\dots (12)$$

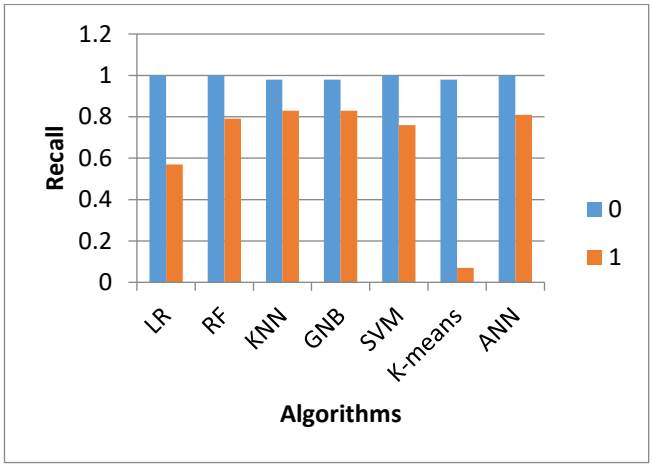
Additionally the accuracy is the ratio of correctly recognized information and total information produced for recognition. The accuracy can be measured using the following equation:

$$\text{accuracy} = \frac{\text{correctly recognized}}{\text{total samples}} \dots\dots\dots\dots (13)$$

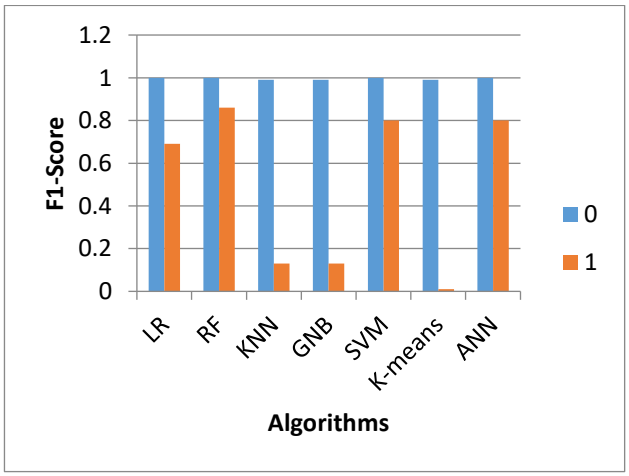
The obtained performance is demonstrated in both manners i.e. graphically using the bar graph and terms of obtained values. The obtained performance is demonstrated in figure 4 and Table 1. Fig. 4(A) shows the precision, Fig. 4(B) shows the recall, the f1-score is given in Fig. 4(C) and Fig. 4(D) shows the accuracy of the models. According to the demonstrated performance the k-means, GNB and KNN provide similar accuracy. These three algorithms are providing 0.98% accuracy.

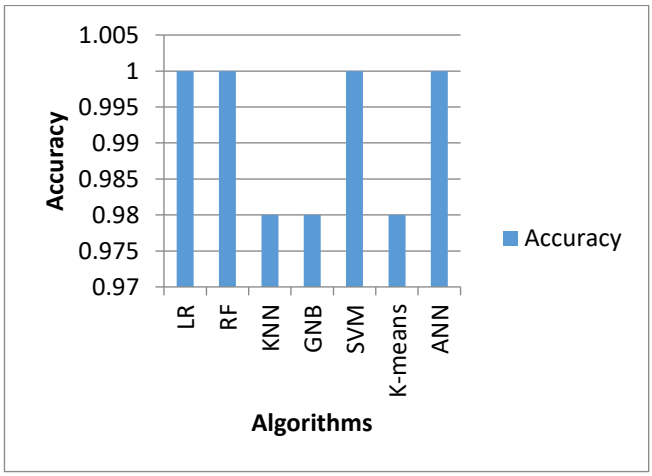
On the other hand, the classifiers SVM, RF, LR, and CNN provide similar accuracy which is a total of 1. Therefore, with the credit card fraud detection problem the SVM, RF, LR, and CNN algorithms are providing higher accurate results.





(A) (B)





(C) (D)

Figure 4: Shows the performance of the implemented machine learning algorithms in terms of (A) precision (B) recall (C) F1-score and (D) Accuracy

Therefore the SVM, RF, LR, KNN, GNB, k-Means and CNN algorithms are compared for their training time. The training time of these algorithms is demonstrated in Fig. 5.In this diagram the X axis contains the algorithms and the Y axis shows the training time of the algorithms in terms of seconds. According to the obtained performance in terms of training time, the algorithms SVM and RF are expensive than the other algorithms.

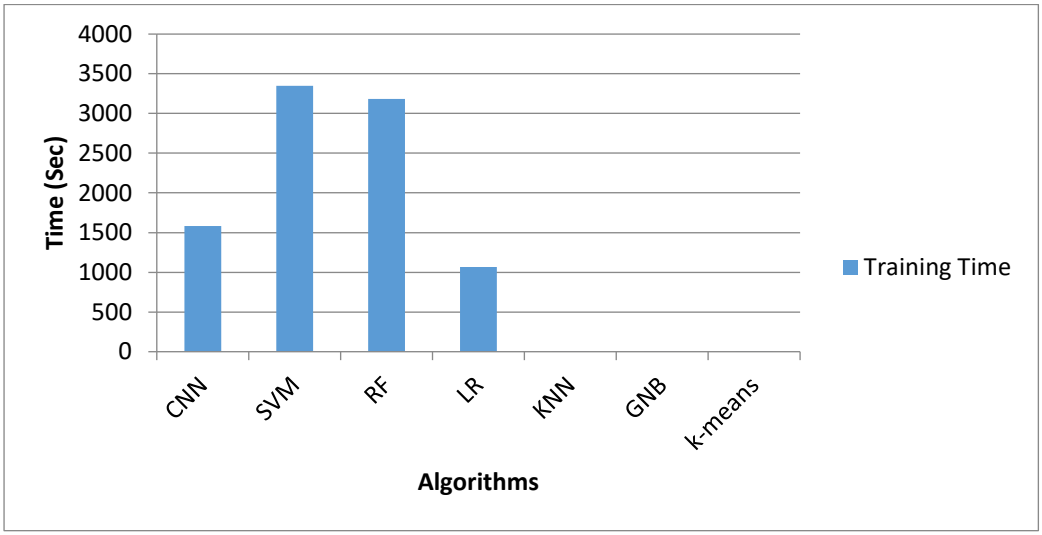


Figure 5: Training Time

Therefore according to the overall performance (i.e. accuracy as well as training time), we can say the CNN and LR are able to efficiently and accurately work on the credit card fraud detection dataset. Thus we recommend using the CNN and LR for future credit card fraud detection modeling.

V. CONCLUSIONS

Credit card frauds are one of the crucial issues for credit card companies. Due to this significant losses are occurred, because credit card companies cannot charge the amount to their consumers which is not used by the consumers. Therefore it is a must to keep monitoring credit card transactions and possible potential frauds. In addition, the cases of credit card fraud are increasing day by day globally. Therefore we need to design an accurate and efficient way of monitoring fraud transactions. However, a number of machine learning-based models are developed recently for this task but most of them are not much effective or accurate.

Thus, in this presented work we proposed to evaluate the different machine learning models which are suitable to apply to credit card fraud detection thus we have selected seven machine learning models namely SVM, CNN, RF, LR, GNB, KNN, and k-means. These models have been implemented using python technology. Additionally, a model has been introduced to process the

information. The consequences of the implemented models are measured and reported in this paper. Based on the obtained results the K-means, KNN and GNB provide similar accuracy which is up to 98%. Additionally, the CNN, SVM, RF, and LR provide higher accurate results which are found up to 100%.

Finally to make a selection of the final machine learning model which is accurate as well as efficient we also measure the training time of the models. Based on the training time we found the SVM and RF is much more expensive and requires up to three times higher time for training as compared to LR and CNN. Thus in near future, the LR and CNN have been considered for preparing the final credit card detection model.

In near future the following extension of the work has been proposed for work:

1. Utilize the CNN and LR for preparing the credit card fraud detection model.
2. Utilize the more and different datasets for validating the proposed model.

REFERENCES

1. Sangeeta Mittal and Shivani Tyagi, "Chapter 26: Computational Techniques for Real-Time Credit Card Fraud Detection", Handbook of Computer Networks and Cyber Security, © Springer Nature Switzerland AG 2020
2. G. Sasikala, M. Laavanya, B. Sathyasri, C. Supraja, V. Mahalakshmi, S. S. Sreeja Mole, Jaison Mulerikkal, S. Chidambaranathan, C. Arvind, K. Srihari, and Minilu Dejene, "An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications", Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 2439205, 12 pages
3. Ibtissam Benchaji, Samira Douzi, and Bouabid El Ouahidi, "Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks", Journal of Advances in Information Technology Vol. 12, No. 2, May 2021
4. V. B. Nipane, P. S. Kalinge, D. Vidhate, K. War, B. P. Deshpande, "Fraudulent Detection in Credit Card System Using SVM & Decision Tree", IJSDR, Volume 1, Issue 5, May 2016
5. K. Gowthami, K. V. L. E. Praneetha, G. Vinitha, Ch. R. Kumari. P. S. Krishna, "Credit Card Fraud Detection Using Logistic Regression", Journal of Engineering science, Vol 11, Issue 4, April/2020
6. S. Kiran, J. Guru, R. Kumar, N. Kumar, D. Katariya, M. Sharma, "Credit card fraud detection using Naïve Bayes model based and KNN classifier", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 4, Issue 3, 2018
7. C. Sudha, T. N. Raj, "Credit Card Fraud Detection in Internet Using K-Nearest Neighbor Algorithm", IPASJ International Journal of Computer Science, Vol. 5, Issue 11, Nov 2017
8. D. Meenakshi. B, Janani. B, Gayathri. S, Mrs. Indira. N, "Credit Card Fraud Detection Using Random Forest", International Research Journal of Engineering and Technology, Volume: 06 Issue: 03, Mar 2019
9. D. Viji, S. K. Z. Banu, "An Improved Credit Card Fraud Detection Using K-Means Clustering Algorithm", International Journal of Engineering Science Invention, e-ISSN: 2319 – 6734, PP. 59-64, NCIOT-2018

10. Y. Abakarim, M. Lahby, A. Attioui, “An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning”, SITA’18, Rabat, Morocco, Association for Computing Machinery, October 24–25, 2018
11. A. Mujumdar, Dr. Vaidehi V, “Diabetes Prediction using Machine Learning Algorithms”, Procedia Computer Science 165 (2019) 292–299
12. N. Rtaylia, N. Enneya, “Selection Features and Support Vector Machine for Credit Card Risk Identification”, Procedia Manufacturing 46 (2020) 941–948
13. P. K. Sadineni, “Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms”, Proceedings of the Fourth International Conference on I-SMAC, 2020 IEEE
14. O. Adepoju, J. Wosowei, S. lawte, H. Jaiman, “Comparative Evaluation Of Credit Card Fraud Detection Using Machine Learning Techniques”, Global Conference for Advancement in Technology (GCAT), 2019 IEEE
15. D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, A. Anderla, “Credit Card Fraud Detection - Machine Learning methods”, 18th International Symposium Infoteh-Jahorina, 20-22 March 2019, IEEE
16. A. M. Rahat, A. Kahir, A. K. M. Masum, “Comparison of Naive Bayes and SVM Algorithm based on Sentiment Analysis Using Review Dataset”, 8th International Conference on System Modeling & Advancement in Research Trends, 22nd–23rd Nov, 2019 IEEE
17. S. Kiran, J. Guru, R. Kumar, N. Kumar, D. Katariya, M. Sharma, “Credit card fraud detection using Naïve Bayes model based and KNN classifier”, International Journal of Advance Research, Ideas and Innovations in Technology, Volume 4, Issue 3, 2018
18. I. Sadgali, N. Sael, N. Sael, “Fraud detection in credit card transaction using neural networks”, SCA2019, CASABLANCA, Morocco, Association for Computing Machinery, October 2–4, 2019
19. T. H. Lin, J. R. Jiang, “Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest”, Mathematics, 9, 2683, 2021
20. Dileep M R, Navaneeth A V, Abhishek M, “A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms”, Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, 2021 IEEE
21. Y. Chen, R. Zhang, “Research on Credit Card Default Prediction Based on k-Means SMOTE and BP Neural Network”, Hindawi Complexity, Article ID 6618841, 13 pages, Volume 2021
22. P. Shanmugapriya, R. Shupraja, V. Madhumitha, “Credit Card Fraud Detection System Using CNN”, International Journal for Research in Applied Science & Engineering Technology, Volume 10, Issue III, Mar 2022