International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

AI Based Credit Card Fraud Detection using Machine Learning Technique

Dr. B. Rajesh Kumar[1]
Department of Software Systems
Sri Krishna Arts and Science College

Sam Ashbal Raj J[2]
Department of Software Systems
Sri Krishna Arts and Science College

ABSTRACT

As the number of companies and consumers using credit card information for financial transactions has grown, which has resulted in a substantial rise in fraud cases. This issue has been made worse by dealing with outliers, unbalanced, and noisy data. This work proposes the use of artificial intelligence for fraud detection. The proposed technique uses logistic regression as a method for creating the classifier in order to avoid transactions using credit cards fraud. Pre-processing ensures a high degree of precision in detection and is employed to control dirty data. The pre-processing stage of cleaning the data uses two distinct basic techniques: the mean-based methodology and the clustering-based strategies. The proposed classifier yields better results in terms of error rate, receptivity, and accuracy.

Keywords **: Credit cards, machine learning, and artificial intelligence**

1. INTRODUCTION

An increasing number of transactions will be made online as the globe moves toward a cashless future. Fraudsters nowadays do not need to be present at the scene of the crime to do it. They have numerous ways to conceal their identity, so they can carry out their evil deeds in the warmth of their own homes. It is challenging to find those who utilise identity concealing techniques such as utilizing a VPN, passing the victim's communication through the Tor network, etc. It is critical to understand the consequences of monetary losses incurred via internet sources. Assuming card details are obtained, fraudsters have two options: either they use the payment cards for personal use or they sell the details of your card to various people, as is the case in India, where the card information of around seventy million individuals is sold through the dark web. One of the biggest credit card fraud incidents in UK history led to GBP 17 million in financial damages. A group of international con artists came together in the second decade of the the decade of 2000 to obtain the credit card information ofover 32,000 accounts. The largest theft of credit cards in history is thought to have occurred in this instance.

Thus, credit card fraud causes billion-dollar losses as a result of insufficient security measures. Card issuers are reassured that each transaction are benign, as are cardholders using their cards and issuers executing the transactions. On the other hand, fraudsters want to trick cardholders and financial institutions into thinking that the unauthorized transactions are real. Furthermore, certain fraudulent transactions take place on a regular basis with the intention of making money without the card issuers' or cardholders' knowledge. The most disheartening thing about payments made with credit cards is that often neither cardholders nor the regulated establishments realise they have been participating in fraudulent behaviours. Because of this, it is often exceedingly difficult to spot a fraudulent transaction among thousands of genuine interactions, especially when there are significantly fewer criminal transactions than lawful ones. The banking and insurance industries can potentially be kept safe from crime by utilising a variety of fraud detection techniques, such as predictive analytics and data mining, especially demonstrating algorithms that employ clustering and anomaly detection techniques. Machine learning algorithms are necessary for most of these techniques, whether supervised or unsupervised, and they are helpful in categorising credit card fraud. However, there are several challenges that machine learning algorithms must overcome in order to detect every scam. An ideal model based on machine learning would need the highest values for common assessment metrics. To come closer to this perfect framework, this field of research has to make a lot of breakthroughs. Numerous components, such as the use of cross-validation techniques for machine learning methods, and resampling strategies, influence the issues associated with credit card fraud detection. These considerations can enhance the model's performance, as the evaluation metrics can attest. In practical applications, balanced datasets are extremely uncommon, hence most of the period the classification algorithm reduces the importance of the minority class within the dataset. In reality, the minority class played a critical role in the classifying process, especially when it came to terms of uncovering fraudulent transactions with credit cards.

The suggested method, which selects the optimal machine learning algorithms first, uses a variety of resampling strategies to highlight the imbalance class issue resulting from the dataset's uneven distribution of classes. This research takes into consideration both improved cross-validation (CV) approaches and resampling strategies. This paper proposes a comprehensive way for choosing both the best machine learning algorithm and the best reproducing strategy. This approach is based on a two-phase research that uses metrics to evaluate performance. Analyzing nine ML techniques with their default settings is the goal of the first step. The nine methods are: There are several gradient booster machines: Using random forest (RF) algorithm, also known as the KNN algorithm), Decision Forest (DT), Naively Bayes (NB), the extreme gradient booster (XGBoost), Lite Gradients boosters Machine (LightGBM), and Classification Boosting (CatBoost). For usage in the second round, only the best three approaches from the initial batch of nine are chosen. In the second step, 19 distinct resampling techniques will be examined using all of the three methods that were established in the previous phase. These 19 resampling methods fall into the following categories: There are eleven undersampling, six oversampling, and two that combine both inadequate sampling and oversampling methods simultaneously. In addition, the goal of this step is to determine which algorithm and reproducing technique combination will yield the best suggested model in terms of overall performance. This innovative method stands out because it looks at many ways to address the issue of class imbalance in the dataset.

This is illustrated by drawing comparisons between the best machine learning techniques, resampling, and using stratified K-fold CV. Utilizing so many diverse approaches and strategies yields a hopeful outcome, especially in light of the actuality that gathering every single one of the assessment metric values took more than a month. The remainder of the written piece was organized in this manner. The second section offers an overview of pertinent literature. In the third part, the recommended approach is described. The final portion is going to address what was discovered during the experiment. A synopsis of the results and recommendations for further study are provided in the fifth section's conclusion.

According to the law, criminal activity is defined as having the intent of misleading individuals with the purpose to benefit financially or personally. Because of this, the two main strategies for preventing loss from fraud are fraud detection and prevention. While preventive fraud prevention is the proactive strategy to prohibit fraudulent activities from arising, catching fraud is the procedure of comprehending fraudulent transactions that are performed by fraudulently persons. These days, it's common to find a range of payment cards, such as financing, charge, debit cards, and prepaid cards. They're the most widely used form of payment in certain nations. It's true that developments in technological advances have opened the door to adjustments in our financial practices, particularly with regard to payment methods, which have shifted from being physical actions to digital ones involving electronics. This has completely changed the environment in which monetary policy is implemented, as well as how big and small businesses operate. using a credit card without authorization to pay for goods or services. These types of transactions can be carried out electronically or physically. The credit card is present physically during physical transactions. Conversely, digital transactions happen over the phone or the internet. Typically, a cardholder gives their credit card numbers, card verification numbers, and expiration date over the phone or on a website. Credit card usage has skyrocketed due to the recent explosive growth in e-commerce.

In Malaysia, there were roughly 317 million credit card interactions in 2011, and by 2018, there were 447 million. According to, credit card theft hit a record $21.84 billion worldwide in 2015. With more people using credit cards, there have been an increasing number of fraud occurrences. Despite the implementation of several verification techniques, there has been little to no decline in credit card fraud instances. Fraudsters have a plethora of options due to the constantly evolving financial services industry and the possibility of significant financial advantages. Payment card fraud proceeds are frequently utilized for illegal actions that are difficult to stop, such financing terrorist attacks. Since they can hide their identity and location online, fraudsters tend to gravitate towards it. The financial industry has been severely impacted by the recent rise in credit card theft. Since merchants are responsible for all costs associated with credit card theft, including fees from card issuers, administrative costs, and other penalties, they are primarily affected. The merchants bear full responsibility for any losses, which results in higher product pricing and lower discounts. Therefore, minimising this loss is crucial. Reducing the amount of fraudulent transactions requires an efficient fraud detection system.

2.RELATED WORKS

Credit card fraud breaks into two categories: external fraudulent and internal fraud. 12, 15] Three different groups have been set up for a more detailed classification: Internet fraudsters (credit card generators, however, website replication, and deceptive seller's pages), merchant-related forgeries (seller a conspiracy and triangulation), and common account-related thefts (realization, stolen, considered takeover, fake, and counterfeit). [16]. According to [17], there were over USD 16 billion in global fraud losses for banks and businesses in 2014. This represents a nearly 2.5 billion United States dollars increase in losses from the previous year. According to the study, there were instances of 5.6 dollars of criminal activity associated with each $100. The main factor that sets apart credit card transaction data is an unusual event. Typically, there are similar features that set lawful and illegal transactions distinctive. Fraudsters pick up cutting-edge methods to imitate real cardholders' banking habits. As a result, the definition of what kind of conduct is honest or unethical continues to evolve. Due to this inherent feature, there are fewer genuine fraudulent cases found in a collection of payment card activity information, which leads to distributions that have a strong bias in favor of the negative group (legal transactions). Twenty percent of the instances that are positive, 0.025% of the positive instances [19], and less than 0.005% of the favorable cases [8] are included in the financial card information examined in [18]. The data employed for the above research demonstrated that 0.172% of all of the transactions belong to the advantageous category (frauds). The severely distorted credit card data has been tested through a number of sampling procedures. [18, 20] employ a random sample technique to explain experimental findings that show classification algorithms with the lowest rates of false positives and the highest true positive rate are produced when training information related to fraud as well as non-fraud is purposefully distributed 50:50.

In the publication [8], stratified sampling is utilized to significantly undersample the legitimate records. The experiment comparing the 50:50, 10:90, as well as 1:99 sample sizes show that the aforementioned 10:90 equivalent matches deception as well as legitimate incidents. most satisfactorily on the basis of efficiency assessments on the 1:99 set since it is most comparable to the actual distributed that contains both legitimate and fraudulent occurrences. In [21], a stratified sampling method is also performed. To maintain important trends from the data gathered, a combination of inadequate sampling failure scenarios and excessive sampling instances that were positive is used in this study.

The basis for identifying credit card fraud is a thorough examination from cardholder habits of spending. This expenditure profile is examined using the best combination of parameters in order to fully capture the unique purchasing patterns of the card's user. Illegitimate transaction activity as well as legitimate usually have dynamic characteristics. Therefore, the best characteristics need to be selected in a way that clearly distinguishes the two profiles in order to categorize transactions made using credit cards efficiently. The effectiveness of fraud with credit card identification systems is influenced on the elements that comprise the history of card usage and the methods employed. These variables are obtained by combining transaction data with a credit card's historical transaction history. Time-based amount data, limited-time volume activities figures, retailer variety statistics, geographical information, and overall transactions statistics are the five main categories into which these variables may be divided [19]. The card's total use profile is displayed by the variables that fall within the broad scope of every transaction's information type. The cardholder's spending habits are displayed by the variables under the locale statistics type, which takes geographic regions into consideration. The factors listed underneath the merchant's statistics type reflect the debit card's usage in several merchant classifications. Each card's application character is defined by the parts of time-based statistics kinds in terms of their utilization values versus instant intervals or usage numbers versus time ranges. The majority of publications emphasised cardholder profiles above card profiles. It goes without saying that a single person can make different types of transactions with many account numbers for credit cards.. As a result, using cardholders allows one to offer a distinct spending profile. Since a cardholder may demonstrate a variety of behaviors across several cards on your own, whereas one transaction on a card can only present a single spending profile, the focus is this investigation is on the card's use rather than the cardholder. Thirty variables are used in [19], (20 variables have been reduced to sixteen relevant ones.

Fraud rates typically rise when credit cards surpass cash as the most widely used form of payment for internet and offline payments. With the introduction of big data, the conventional human approaches to fraud detection are growing more difficult due to their imprecise and time-consuming nature. But these days, financial companies are employing cunning tactics. Computerized intelligence (CI) is the foundation of these intricate deception techniques. Supervision and unsupervised techniques make up the two primary groups of analytical fraud detection methods [22]. In managed techniques for authentication, abnormality transactions are recognized as possible instances of false actions when performing unsupervised fraud identification, while models have been built and computed upon samples of honest and bogus deals [13] to categorize recent activities as dishonest or lawful. You may find an extensive review of both supervised and unsupervised methods in [23]. Identifying bogus credit card purchases has been the focus of numerous studies employing various methodologies.

2.1 EXISTING SYSTEM

Furthermore, earlier systems had issues in real-time settings. These issues relate to the identification of credit card fraud. These issues include data that is unbalanced, noisy, and pertains to drift. The bag construction method, which comprises using the collected data to perform a real-time procedure for sampling, was employed by the authors to address the data issues. They used logistic regression to effectively manipulate noisy data in order to clean it up. To address the idea of drift, a strategy based on incremental learning was suggested.

3. METHODOLOGY

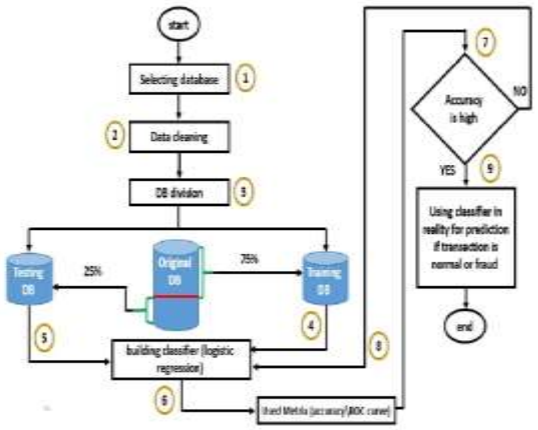

start
Selecting database
1
2
Data cleaning
DB division
3
Testing DB
25%
Original DB
75%
Training DB
4
5
building classifier (logistic regression)
6
Used Metrics (accuracy/ROC curve)
8
7
Accuracy is high
NO
YES
9
Using classifier in reality for prediction if transaction is normal or fraud
end

Figure 3.1 Overall Proposed Architecture

3.1 DATA SET DESCRIPTION

The The University of Louisiana at ML Group provided the dataset, and they also have an explanation. The dataset includes credit card purchases made in September 2013 by consumers across Europe. A total in 284,807 transactions over the course of two days are included in this dataset. The positive class, which makes up 0.172% of the bank transaction data, is comprised of fraud events. There is a noticeable imbalance in the statistics, skewed in favor of the healthier class. Its sole input variables are quantitative (continuous), obtained by transforming a feature set using basic component analysis (PCA) and producing 28 principle components as a result. Therefore, a total of thirty input characteristics are used in this investigation. Security issues hinder the specifications and context of the features from being disclosed. The seconds that pass between each trade and the dataset's initial transaction are included in the time feature. The total amount of the transaction is shown by the 'amount' feature. When there is no fraud present, the binary classification's targeting class, feature "class," receives a value of 0, and when there is fraud present, it receives a value of 1. (a scam).

3.2 DATA PRE-PROCESSING

At this stage, the data needs to be cleaned up and prepared for the classifier's training phase. Real-world data are typically noisy. As such, a cleaning procedure is required. The steps involved in an information cleansing process are as follows:

1The absence of digits should be entered. An input error caused a cell with an absent answer inside an elected record to be empty..

2) Address any discrepancies. This implies that a data collision needs to be fixed if it occurs.

3) Remove any irregularities. Outliers are quantities that are abnormal, such as levels that are disproportionately high or low.

Fortunately, with the exception of a few missing numbers, the majority of the data utilized in the set of numbers are cleansed. and outliers.

Since the data are numerical, the method for addressing the missing values is based on the mean (a mathematical process). gives an illustration of how to enter the missing value. To deal with outliers, a clustering-based method is applied in this work. The basic idea is to create three clusters: one for the typical data, one for high computation, as well as one for low values. The final two clusters—those with outliers—are eliminated once the data has been grouped into clusters. The Outlier Removal Mechanism.

3.3 FEATURE EXTRACTION

We will distribute the goal value in this part, which is essential for selecting relevant accuracy metrics and, as a result, correctly evaluating various machine learning models. Counting values of the explanatory variable, often referred to as the deciding variable, will be the first step in determining whether or not a transaction involving credit card fraud is fraudulent. Secondly, we will distinguish between category and numerical features. Next, we will illustrate the relationship between the category features in a variety of plots and attempt to determine—or rather, observe—the impact of those qualities on the actual determining variable, or “outcome.".

3.4 TRAIN THE MODEL

LOGISTIC REGRESSION

Using a functional approach, logistic regression calculates the likelihood of a binary response. based on many factors (features). It ascertains which parameters best fit the sigmoid, a nonlinear function. The sign geometry function (σ) and the algorithm's input (x).

$$\sigma(x) = \frac{1}{\left(1+\ell^{-x}\right)}$$

$$x = w_0 z_0 + w_1 z_1 + \ldots + w_n z_n$$

For every member of the the vector (z) that carries the entered data, the optimal parameters (w) are multiplied. to obtain the target class's classification classification. The output of this operation is a single integer. If a sigmoid's value is more than 0.5, it's considered a 1, else it's considered a 0. To find the best-fit parameters, a classification system is trained applying an optimization approach. Experiments were carried out to evaluate the classifier's performance utilizing improved randomly distributed gradient-descending optimization techniques and valley elevation (9).

$$w := w + \alpha \nabla_w f(w)$$

where the parameter Δ represents the changing magnitude of the incline ascent.. Until a halting condition is satisfied, the processes are repeated. To find out if the criteria are converging, the optimization techniques are examined throughout iterations ranging from 50 to 1000. In other words, do the parameters approach a fixed value or do they vary continuously? After 100 repetitions, steady variables are attained. Instead of updating the classifier all at once when new information has been received, stochastic gradient ascent does so gradually. At the beginning, the ratios are all set to

1. The ascent from the gradient is then computed for each feature recurrence in the dataset. The gradient is multiplied by alpha to update the weights vector. The weight scalars is then returned after that. Because stochastic gradient ascent modifies weights one example at a time and is computationally efficient, it is appropriate for the large amount of data in our study.

ALGORITHM PROCEDURE

Step 1. Model formulation:

Describe the independent variables (elements influencing the outcome) and the variable that's dependent (binary outcome you wish to predict).

Select the sigmoid activation function (1 / (1 + exp(-z))), for illustration. This function converts the linear sum of characteristics and weights (z) to a value (which indicates the likelihood that the event will occur) between 0 and 1.

Step 2. Optimization:

The algorithm minimizes a loss function (such as log loss or cross-entropy) by iteratively optimizing the model parameters (weights). This quantifies the difference between the actual result in binary terms and the anticipated probabilities of the model. Gradient descent and other optimization techniques are used to gradually improve the model's ability to predict the binary decision by adjusting the weights in an area that minimizes the loss.

Step 3. Prediction:

The theory can be employed to perform prediction once it has been trained. The model uses the sigmoid function and weighted sum to calculate the probability of an event happening for the latest information with its attributes. The outcome is generally characterized using a threshold value, usually 0.5; a forecast possibility exceeding the threshold is categorized as positive (an event is occurring), while a predicted probability below the cutoff is labeled as negative (an event is not occurring).

Step 4. Evaluation:

Recall, precision, repeatability, and F1-score are among the metrics utilised to assess the model's performance. These measures evaluate the degree to which the projections made by the model and the actual results agree.

3.5 TEST MODEL

We test our framework's hypothesis using this portion of the dataset. It remains unaltered and hidden until the equations and hyperparameters are determined. Only then is the model used to test data to obtain a precise estimation of its performance when applied to real-world data.

4. RESULT AND DISCUSSION

The calculation of precision involves dividing the entire number of predictions made for a dataset by the entire amount of the correct predictions. It may immediately inform us of a model's training success as well as the overall performance trajectory that the model may follow. It does not, however, offer precise information on how it relates to the issue. The accuracy, or a PPV, is an acceptable measure of outcomes even while rate of false positives are considerable. Turnover is the model measure that determines which model is best when one considers a large cost connected to false negatives. Recall is beneficial, even when false negatives come at a high expense. To determine symmetry along recall and accuracy, you need to get an F1-score.It works as a broad indicator of the degree of precision of the model. It blends memory with accuracy. It is possible to explain a high F1-score by having few negative results and few fraudulent positives.

True Positives (TP):- These are the positive numbers that were correctly predicted, indicating that both the real and projected outcomes for the class are yes.

True Negatives (TN):- These negative numbers demonstrate that the actual and predicted values for the class are both a value of zero proving thus the prediction was accurate.

Values that appear when the predicted class as well as our actual class diverge are known as fake negatives and false positives

False Positives (FP):- When the class anticipated is yes but the true classification is no, this is known as a false positive (FP).

False Negatives (FN):- False Negatives (FN): Arrangements for scheduled sessions where instruction is not provided.

$$\text{Accuracy} = \frac{(TP + TN)}{(TN + FN) + (FP + TP)}$$

$$\text{Recall} = \frac{TP}{(FN + TP)}$$

$$\text{Precision} = \frac{TP}{(FP + TP)}$$

$$\text{F1} - \text{measure} = 2 \times \frac{(\text{Precision} \times \text{Recall})}{(\text{Precision} + \text{Recall})}$$

Where,

- Correctly recognized (TP) means true positive
- Erroneously detected as a false positive (FP)
- Correctly dismissed True Negative (TN)
- An inappropriate acceptance is usually referred to as a false negative (FN)..

ACCURATE

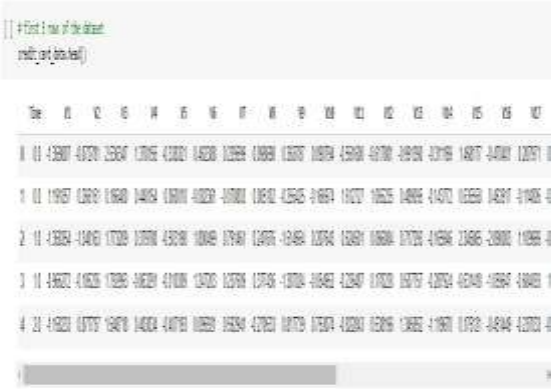
Specifically, one must ascertain the proportion of Forecasts for the positive subclass that accurately represent the positive class.

Reliability = TP/TP+FP

RECALL

The number of accurately predicted groups that are positive among all the positive samples in the dataset is referred to as "recall".

Recall = TP/TP+FN



```
# First 5 rows of the dataset
credit_card_data.head()
```

Figure 4.1 SCREENSHOT FOR DATA SET

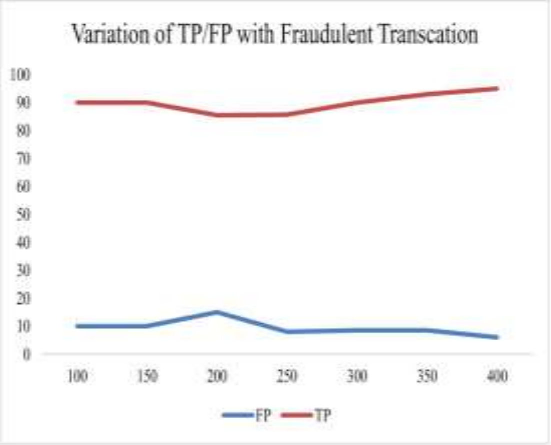
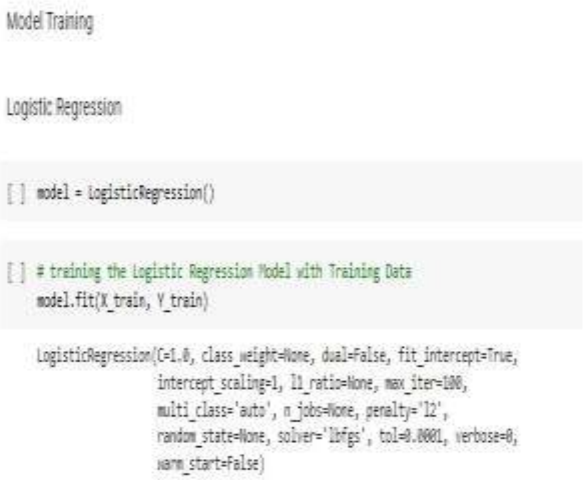


Figure 4.2 Graph Representation for Fraudulent Transaction



Model Training

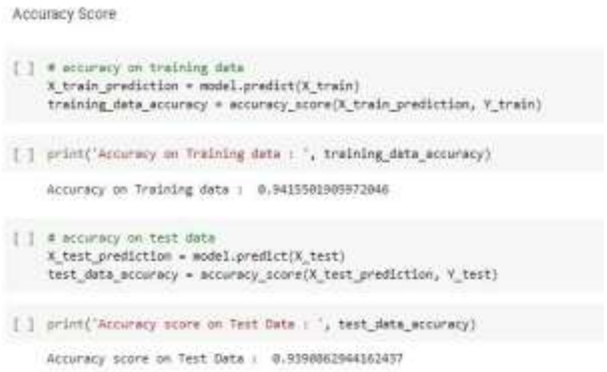
Logistic Regression

```
[ ] model = LogisticRegression()
```

```
[ ] # training the Logistic Regression Model with Training Data
    model.fit(X_train, Y_train)

    LogisticRegression(C=1.0, class_weight=None, dual=False, fit_intercept=True,
                       intercept_scaling=1, l1_ratio=None, max_iter=100,
                       multi_class='auto', n_jobs=None, penalty='l2',
                       random_state=None, solver='lbfgs', tol=0.0001, verbose=0,
                       warm_start=False)
```

Figure 4.3 Screen Shot Model training



Accuracy Score

```
[ ] # accuracy on training data
    X_train_prediction = model.predict(X_train)
    training_data_accuracy = accuracy_score(X_train_prediction, Y_train)
```

```
[ ] print('Accuracy on Training data : ', training_data_accuracy)

    Accuracy on Training data :  0.9415501905972046
```

```
[ ] # accuracy on test data
    X_test_prediction = model.predict(X_test)
    test_data_accuracy = accuracy_score(X_test_prediction, Y_test)
```

```
[ ] print('Accuracy score on Test Data : ', test_data_accuracy)

    Accuracy score on Test Data :  0.9390862944162437
```

Figure 4.4 Screen Shot For Accuracy Score

5. CONCLUSION

The detection scientific credit card fraud is a crucial field of study. Financial institutions are reporting a rise in fraud cases, which is the cause of this. This issue opens the door to developing fraud detection systems with artificial intelligence. An automated intelligence (also known as AI fraudulent activity detection system's machine learning algorithm, also known as a classifier, requires training from a database. Actually, there are outliers, noisy information, and values that are not present in the tainted data. The accuracy rate of the system is negatively impacted by these issues. The above issues are thought to be resolved using a logistic regression-based classifier. The recommended classifier is evaluated using metrics such as sensitiveness, accuracy, and the rate of error. In comparison to the proposed logistic regression-based classifier, two commonly used classifiers are examined: the vote classifier and the K-nearest peers classifier. The logistic regression-based classifier, with accuracy of 97.2%, responsiveness of 97%, and inaccuracy rate of 2.8%, yields the best results.

REFERENCES

[1]. Maes, S., Tuyls, K., Vanschoenwinkel, B. and Manderick, B., (2022). Credit card fraud detection using Bayesian and neural networks. Proceeding International NAISO Congress on Neuro Fuzzy Technologies.

[2]. Ogwueleka, F. N., (2021). Data Mining Application in Credit Card Fraud Detection System, Journal of Engineering Science and Technology, Vol. 6, No. 3, pp. 311 – 322.

[3]. RamaKalyani, K. and UmaDevi, D., (2019). Fraud Detection of Credit Card Payment System by Genetic Algorithm,International Journal of Scientific & Engineering Research, Vol. 3, Issue 7, pp. 1 – 6, ISSN 2229-5518.

[4]. Meshram, P. L., and Bhanarkar, P., (2019). Credit and ATM Card Fraud Detection Using Genetic Approach, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 10, pp. 1 – 5, ISSN: 2278-0181.

[5]. Singh, G., Gupta, R., Rastogi, A., Chandel, M. D. S., and Riyaz, A., (2018). A Machine Learning Approach for Detection of Fraud based on SVM, International Journal of Scientific Engineering and Technology, VolumeNo.1, Issue No.3, pp. 194-198, ISSN : 2277-1581.

[6]. Seeja, K. R., and Zareapoor, M., (2014). FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining, The Scientific World Journal, Hindawi Publishing

Corporation, Volume 2018, Article ID 252797, pp. 1 – 10, http://dx.doi.org/10.1155/2014/252797

[7]. Patil, S., Somavanshi, H., Gaikwad, J., Deshmane, A., and Badgujar, R., (2018). Credit Card Fraud Detection Using Decision Tree Induction Algorithm, International Journal of Computer Science and Mobile Computing (IJCSMC), Vol.4, Issue 4, pp. 92-95, ISSN: 2320-088X.

[8]. Duman, E., Buyukkaya, A., & Elikucuk, I. (2019). A novel and successful credit card fraud detection system implemented in a turkish bank. In Data Mining Workshops (ICDMW), 2013 IEEE 13th International Conference on (pp. 162-171). IEEE.

[9]. Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2019). 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.

[10]. Ng, A. Y., and Jordan, M. I., (2021). On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes. Advances in neural information processing systems, 2, 841-848.

[11]. Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2022). Credit card fraud detection using Bayesian and neural networks. In Proceedings of the 1st international naiso congress on neuro fuzzy technologies (pp. 261-270).

[12]. Shen, A., Tong, R., & Deng, Y. (2018). Application of classification models on credit card fraud detection. In Service Systems and Service Management, 2007 International Conference on (pp. 1-4). IEEE.

[13]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2019). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.