DOI: https://doi.org/10.17762/turcomat.v11i1.13590

Analysis of Fraud Detection on Credit Cards using Data Mining Techniques

Kiran Kumain
Department of Computer Science & Information Technology,
Graphic Era Hill University, Dehradun Uttarakhand India 248002

Abstract

Credit cards are widely used and accepted in the financial sector all over the world. The latest trend is to use electronic payments and to go cashless. Unfortunately, these credit card-based online transactions and cashless payments invite online fraudsters, who then attack all forms of online payment, including shopping sites and banking services. According to polls, approximately 4 billion people are presently affected by credit card fraud detection, and by 2025, that figure is projected to increase to 8 billion. Concern for its detection has increased as a result of this worrying pace. Both research scholars and industry experts have contributed their effort in this area for this goal. When considering the credit card detection method, its detection largely becomes a difficult problem. Due mostly to its unstable nature and dependence on customer behaviour, and secondarily because the dataset is readily available and easily accessible. This causes the dataset to become imbalanced, which makes it harder for a researcher to find instances of credit card fraud. Implementations of data mining algorithms are suitable for overcoming such difficulties. As a result, applying the proposed thesis necessitates using the random forest, decision trees, logistic regression, and Naive Bayes. The paper also proposes the use of a stacking algorithm, which integrates the basic theories of decision trees, logistic regression, and random forests, in addition to datamining techniques. According to experimental study of the aforementioned classifiers, the stacking algorithm produced an optimum model with exact precisions and generated the greatest accuracy of 97.78%.

Keywords: data mining, electronic payment, fraud detection

Introduction

Nowadays, credit cards have been widely adopted. Such an acceptance is typically made to complete online transactions without using cash. The primary means of transaction is the internet, which makes such transactions possible anywhere. Yet, as this form of payment grows in popularity, it has created new doors and chances for hackers and other criminals to assault the means of exchange. Such assaults eventually result in fraud that happens elsewhere, leaving the entire credit card system exposed to danger. These attacks, coupled with an increase in user concern over the security of their financial information online, highlight the need for a strategy to safeguard customers' personal information from intrusive users and further guard against credit card threats to databases. When a transaction is examined to see if it is valid or not at the terminal, the process of identifying fraud using a classifier model begins. The same is seen in Figure 1 below.

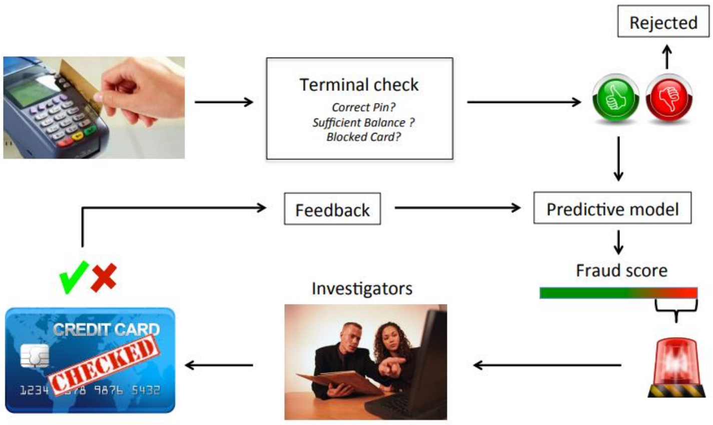


Figure 1: Detection of credit card frauds using predictive models

The terminal point's validation is carried out based on a number of factors, including the customer's bank account balance, the PIN number the user submitted, his login information, etc. The process of a financial transaction starts once all of the necessary requirements have been verified. The predictive model will score these instances of validated transactions and categorise them as legitimate or fraudulent [1]. To achieve this, each transaction with low and high fraud risk is given a score. The investigator, on the other hand, conducts a manual investigation of the same, in which he looks for specific fraud alerts and provides feedback as to whether they are true positives or false positives, allowing the predictive model to be repeated and the system's overall performance to be improved. It is important to highlight that a predictive model can also be created using expert knowledge, although doing so would need for physical supervision and could delay detection. The process is mostly automated for this purpose utilising classifiers that uses data mining techniques. While a deep learning classifier uses the dataset to implement the dataset on hidden layers of the network, a data mining based classifier uses insights from past experiences and allows the prediction to be made using specific parametric functions.

By assuming specific methods, these learning techniques aid in the detection of fraud by keeping an eye out for odd cardholder behaviour. The frequency of credit card thefts has been observed in a variety of ways, from the use of stolen cards to credit card frauds occurring during online transactions. The growth and development of technology has also inspired fraudsters to use novel strategies and tactics. For instance, someone who wants to commit fraud only needs access to a customer's credit card information on a shopping website. Due to the everyday widespread usage of credit cards, the prevalence of these scams has increased exponentially. Clients, banks, and credit card users are now more worried as a result of this. Customers who are involved in situations where the bank could lose money typically pay high rates of interest and membership fees. Due to this, the customer loses faith in both themselves and the associated money transfer method. He could be hesitant to conduct financial transactions online as a result. On the other side, a scam of this nature damages the reputation of the participating bank. When it comes to online stores, it could have an effect on the manufacturer's or retailer's reputation. This causes the client to lose faith over time, which causes a non-financial loss for the manufacturer.

Any financial deception must be discovered before it may manifest. It becomes a study challenge to estimate the number and figure of such frauds in such a situation because financial institutions and banks do not divulge the actual number and numbers. Estimating the frequency of frauds that go undetected can be just as difficult as true fraud detection. This category includes all frauds that go undiscovered and unreported. A problem with data imbalance was also observed while the intended investigation was being carried out. The final distribution of the dataset appears to be unbalanced since the distribution of fraudulent instances is more likely to label it as a true positive fraud case. This affects the system model's overall performance during the training and testing phases and may result in outputs that are generated in error. In addition to any technical difficulties that may arise during the fraud detection process, client behaviour must also be highlighted. It is necessary to regularly monitor his financial transaction graph. Unfortunately, this work gets difficult when used in real time. Another issue with the research is that the amount of attacks that actually happen online tends to be far lower than the prevalence of frauds. It becomes very challenging to stop attacks when there are so many of them going unchecked. In addition to research academics and software developers not being aware of the true numbers, another problem with technological improvements plays a significant role by pushing fraudsters to try various tactics. Major fraud cases in this situation frequently go undiscovered and are only discovered after the customer has suffered financial loss.

Literature Survey

This part of the research provides a concise summary of the most recent research and development in the field of credit card fraud detection, which has been carried out by a variety of academic researchers.

A. Balancing an Imbalance Dataset

In order to avoid an imbalance and ensure that the data is evenly distributed between fraudulent and non-fraudulent cases, sampling techniques are mostly employed to balance the dataset. The sampling approaches do not take into account removing or adding any more information; rather, they match the data to the sample size and make the system simple to execute [2].

As opposed to the first two, oversampling entails growing the class size, which eventually results in a reduction in class disparity as proposed by authors in [3]. By replicating the previous dataset in this manner, the minority class is removed and the incidence of fraudulent and non-fraudulent instances is roughly equal. Oversampling, on the other hand, frequently leads to overfitting and is further addressed by minority class detection. Hence, a sampling technique known as SMOTE is utilised to correct the dataset's imbalance. SMOTE typically interpolates between minority class samples from the existing dataset and replicates those samples [3]. Hence, utilising SMOTE, the model's overall accuracy is improved and the shortcomings of the current system are removed. According to the author's research study in [4], an imbalance in the dataset decreased the system model's performance efficiency. He suggested using machine learning techniques like SVM, random forest, and KNN for this purpose. Although the model's overall effectiveness increased, the problem of data imbalance remained. Authors in [5]; and [6]; also submitted their work in the same domain and encountered issues with an unbalanced dataset in a comparable work proposed by those authors.

The authors saw a significant imbalance where the dataset distributed incorrect predictions. In the sample, there were much fewer non-fraudulent transactions than fraudulent ones. More fake cases than legitimate ones were present in the distributions. The algorithms that the authors employed in this situation provided incorrect forecasts with inaccurate precisions. The authors mostly used ANN, linear regression, and SVM as their algorithms. 17 hidden layers of neurons were created as a result of using ANN as the neural network. Less difficult computations and slow time consumption were used in the implementation.

Authors in [7] presented their research and used six machine learning classifiers to conduct a comparative analysis. An evaluation utilising data mining methods was also part of the implementation. The machine learning-based techniques involved the use of Naive Bayes, SVM, KNN, neural networks, decision trees, and random forests. The initial collection of the two-file dataset came from the Kaggle repository. Regarding both fraudulent and non-fraudulent situations, the files contained training and testing data. The pre-processing and data visualisation processes were completed. It was found that using neural networks to implement the system generated output that was as accurate as possible to the maximum extent. The experiment with neural networks for identifying and categorising credit card frauds was also concluded by the author. In addition, the author noted that the classifier that used Naive Bayes as the algorithm worked slowly and at a high computational cost. It was also noted that the generation of the precision factor was less than the accuracy. As a result, neural network was deemed the best model.

B. Data Mining Methods

Authors in [8] suggested employing machine learning techniques to detect credit card fraud. The data was pre-processed before the algorithms were applied. After the dataset was downloaded from the appropriate repository, it was cleaned, checked for duplication, and any unnecessary information was removed. This resulted in a limited amount of data for machine learning algorithms to work with. The KNN, SVM, and logistic regression machine learning techniques were used by the authors to execute his work. First, the concerns with data imbalance were rectified, and a nice example of data visualisation was seen. The author also suggested CNN as the neural network with 21 layers of hidden neurons in addition to the three machine learning algorithms that were previously mentioned. The system model's overall correctness was improved and a precision of 78.96% was reached as a result of the use of hidden layers.

A decision tree was employed in a theory that the authors in [9] suggested that was based on a working probability algorithm. A voting system was used to create decision trees, and the class receiving the most votes was chosen as the optimum classifier. The author also suggested the development of three classifiers based on machine learning and one stacking-based technique in addition to the voting classifier. The hybrid classifier's use of stacking produced a maximum accuracy of 82.35 percent and resulted in the development of an improved model. A filtered dataset was obtained after the overall implementation of credit card fraud detection was completed.

The execution of seven machine learning algorithms, as well as the executional theory of neural networks, was proposed by authors in [10]. The theory of hidden layers was achieved with seven ML-based classifiers. The dataset, which included both fake and legitimate data, was collected by the author via the Kaggle repository. The dataset was initially divided into training and testing portions for ease of use. Data were discovered to be split 80% to 20%. Also, the author used SMOTE techniques, which assisted in resolving the dataset's data imbalance. SMOTE helped to distribute data equally and filtered out unnecessary information. Eventually, unneeded columns were removed as a result of this. The filtered dataset was subsequently employed in machine learning algorithms, and the system's effectiveness was assessed using metrics including accuracy, precision, and recall factors.

Authors in [11] suggested using only logistic regression and SVM to predict and identify credit card fraud incidents. The same dataset may further categorise the obtained train and test files as fraudulent and non-fraudulent. The authors also included the SMOTE implementation and feature selection methodology. SMOTE was employed to correct the dataset's imbalance. Machine learning classifiers were fed with a balanced distribution of fraudulent and non-fraudulent examples so that their performance could be assessed and an improved model could be created. The feature selection process was completed by the authors using random forest in addition to SMOTE, where only the pertinent characteristics were chosen and the rest were eliminated to maintain overall efficiency.

Implementation Details

In order to categorise credit card fraud detections (CCFD) and further prevent it, it is necessary to look for regular financial activities. Finding fraudulent assaults and accurately classifying them further becomes a difficult issue for any human investigator as data volume grows exponentially. This is the essential justification for the inclusion of technologies like machine learning and deep learning, which allow for the extraction of significant patterns and the exact declaration of results. It can be seen from the literature review done in the previous section that a variety of tactics and approaches might be employed to deal with the problems caused by CCFD. A common baseline of CCFD can be created with the publication of numerous studies in the same field [12]. Starting point can be thought of as the suggested model's system design. The background of the same is explained in Figure 1 below:

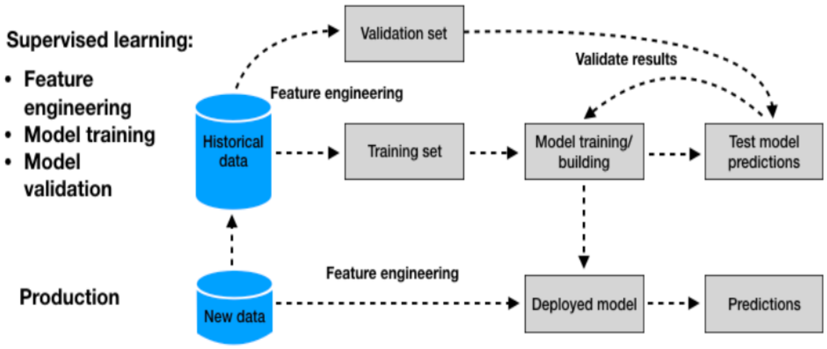


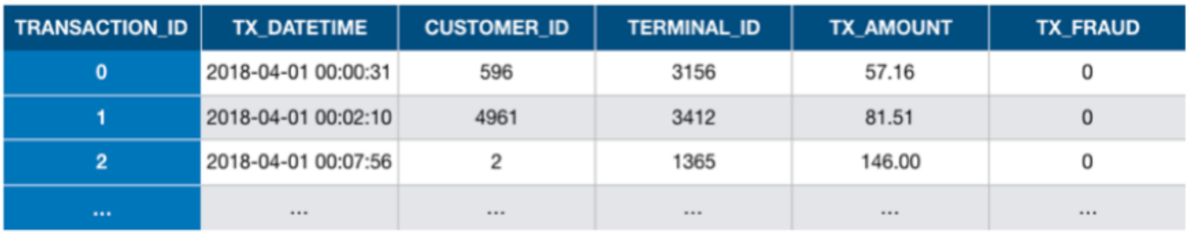
Figure 2: Prediction of CCFD using Data Mining

The dataset from repositories that contain accumulated fraudulent transactions from banks and various payment sectors is collected first as part of the architecture of the system design. The dataset includes data about financial transactions. Such a database of financial transactions can also be divided into the following characteristics:

- Account-related features, such as the user's account number, information on his card limit, the account opening dare, the CVV, etc.
- Financial transaction aspects, such as data on the amount being transferred, the time of the transaction, the recipient's identity, etc.

Following the dataset's gathering, feature engineering methods are used, and the data is then input into the training of data mining classifiers. After this process is finished, the dataset is verified and tested to see what the outcomes are. In contrast to historical data, the same feature engineering process is carried out on the dataset and training is carried out when new data is uploaded into the database. The model is eventually put to use for prediction when it has been implemented.

A customer executes a transaction at a certain point during its actual execution. In the back end of the system model, all transactions are recorded in the database and constitute a collection of historical data. Figure 3 illustrates the storing of historical data as records.



TRANSACTION_ID	TX_DATETIME	CUSTOMER_ID	TERMINAL_ID	TX_AMOUNT	TX_FRAUD
0	2018-04-01 00:00:31	596	3156	57.16	0
1	2018-04-01 00:02:10	4961	3412	81.51	0
2	2018-04-01 00:07:56	2	1365	146.00	0
...	...	...	...	...	...

Figure 3: Historical database of CCFD

It is vital to presume the authenticity of all monetary transactions in order to detect the emergence of frauds. This is done so that the system model can determine whether the data is legitimate or fake. A binary labelization process occurs in which 0 represents a legitimate transaction and 1 represents a fraudulent transaction. There are three stages to the system design for Machine Learning-based implementation:

- Creating a system model from scratch based on previous data
- Using Machine Learning-based classifiers to predict the system model
- Model evaluation using performance metrics

The major purpose of the methodology is to develop a system model that can anticipate the occurrence of credit card fraud during online transactions. So, the research focuses on putting the ideas stated in the previous section into practise to achieve this goal. The entire study technique, however, is provided in this part of the paper. The workflow of the investigation is depicted in Figure 4 below:

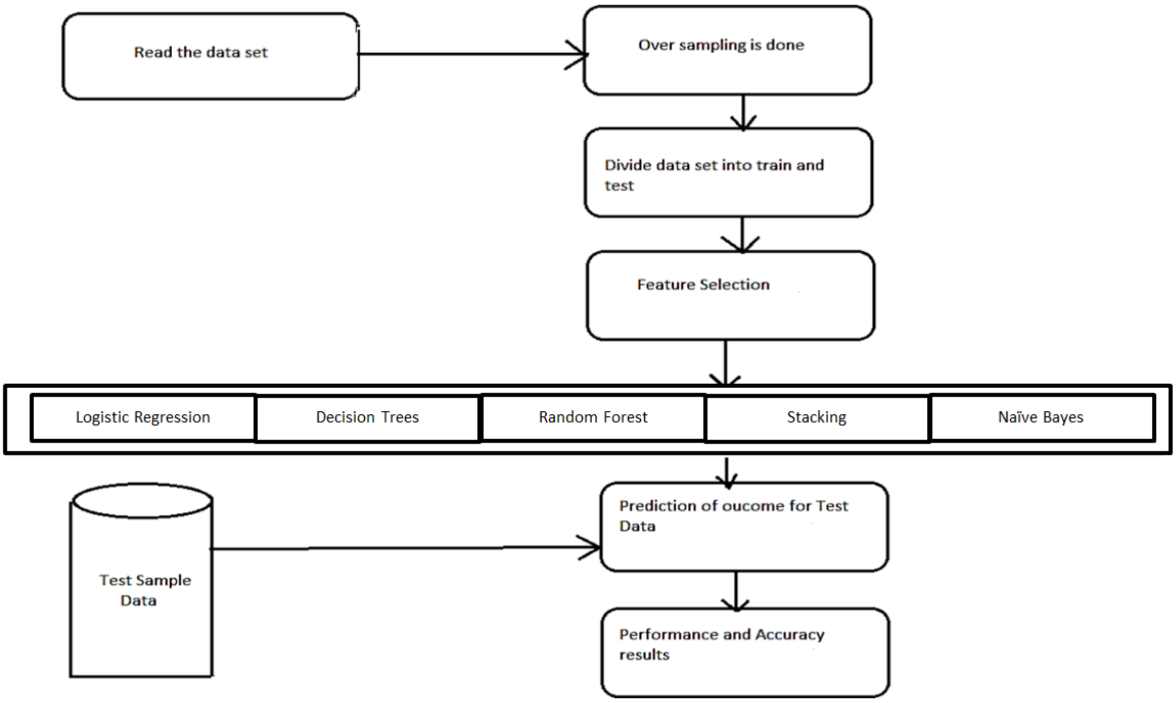


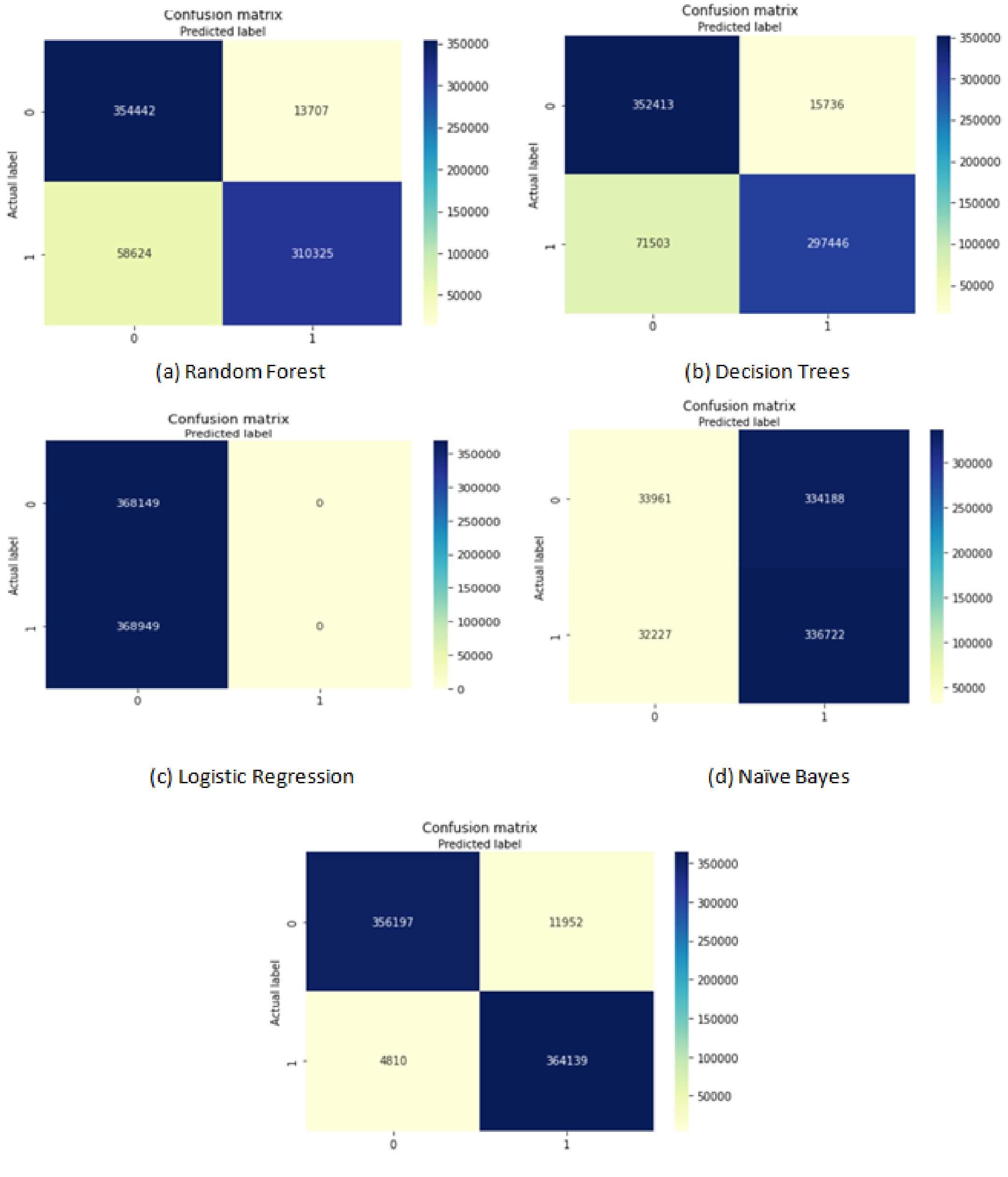
Figure 4: Workflow of Proposed Methodology

The research workflow starts with data collecting from the Kaggle repository in the first step. The dataset is then pre-processed in which the resulting data is balanced using SMOTE. The data is then extracted and selected for filtering redundant data in the following stage. In this stage, the data is viewed using a data visualisation technique and then partitioned using four data mining techniques and one stacking algorithm. The classifier-generated test data is then forecasted for CCFD and evaluated using efficiency metrics.

Results

A. Data Mining Techniques generating Confusion Matrix

In order to derive the confusion matrix that is presented below, a total of four data mining algorithms and one stacking method are carried



(a) Random Forest

(b) Decision Trees

(c) Logistic Regression

(d) Naïve Bayes

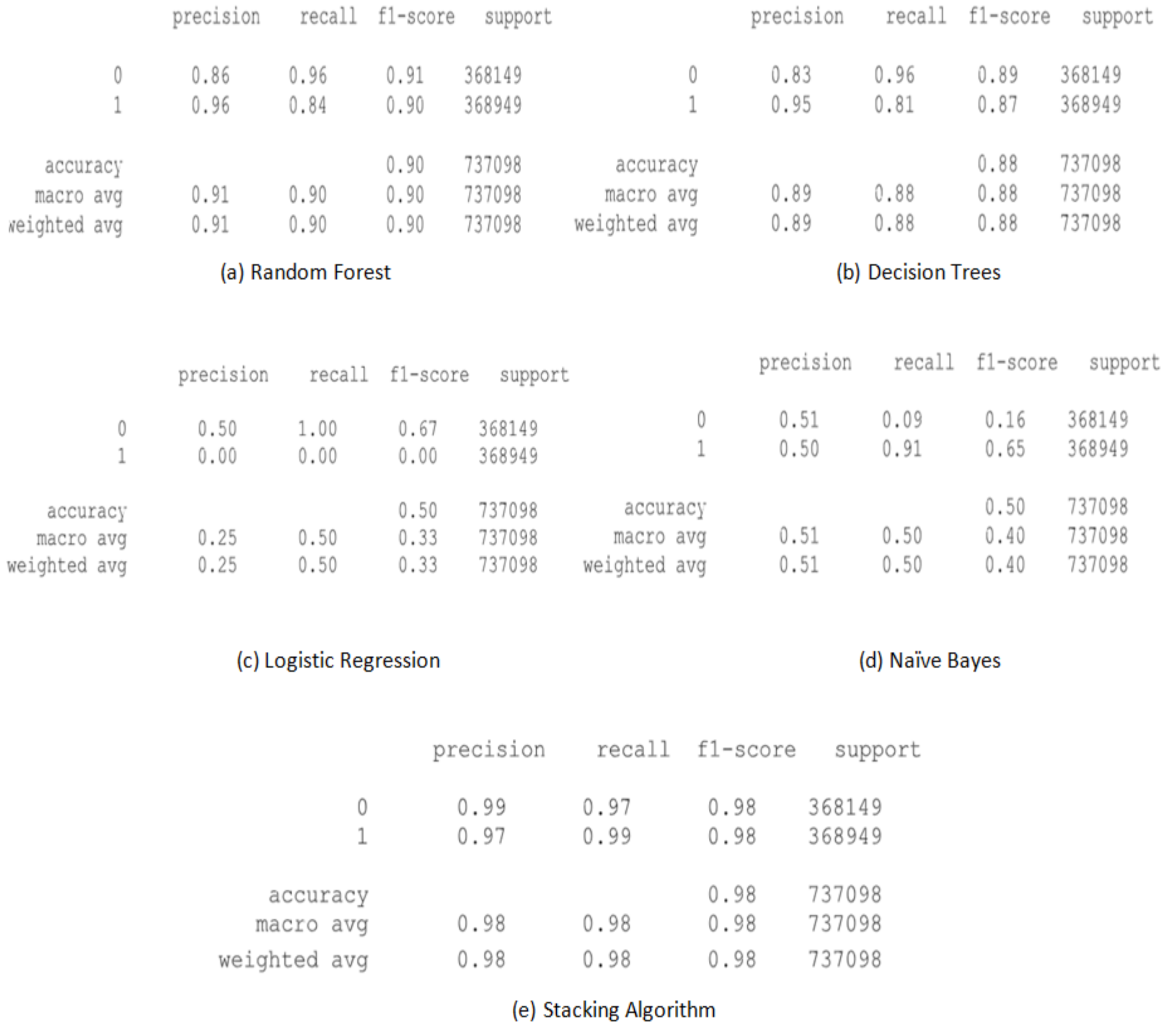
(e) Stacking Algorithm

Figure 5: Confusion Matrix

Figure 5 depicts the confusion matrix of all machine learning classifiers utilised in this study. The values generated by random forest are represented by true negative (TN) values obtained from 5 (a). In this circumstance, TN produces an output value of 35442 cases.

- The TN value thus acquired illustrates that 345442 instances were tested to be fraudulent cases, whereas they were not fraudulent (genuine) cases in actuality (actual). Similarly, the TP value looks to be 310325
- The TP value thus acquired illustrates that 310325 instances were tested to be fraudulent cases, and they were in fact (actual) fraudulent cases
- The FN value thus produced shows that 58624 instances were evaluated and found to be non-fraudulent (genuine), whereas they were fraudulent (actual)
- The FP value so generated illustrates that 13707 occurrences were tested to be fraudulent cases, but in actuality (actual), they were not

B. Data Mining Techniques generating Classification Report



```
              precision    recall  f1-score   support

           0       0.86      0.96      0.91    368149
           1       0.96      0.84      0.90    368949

    accuracy                           0.90    737098
   macro avg       0.91      0.90      0.90    737098
weighted avg       0.91      0.90      0.90    737098
```

(a) Random Forest

```
              precision    recall  f1-score   support

           0       0.83      0.96      0.89    368149
           1       0.95      0.81      0.87    368949

    accuracy                           0.88    737098
   macro avg       0.89      0.88      0.88    737098
weighted avg       0.89      0.88      0.88    737098
```

(b) Decision Trees

```
              precision    recall  f1-score   support

           0       0.50      1.00      0.67    368149
           1       0.00      0.00      0.00    368949

    accuracy                           0.50    737098
   macro avg       0.25      0.50      0.33    737098
weighted avg       0.25      0.50      0.33    737098
```

(c) Logistic Regression

```
              precision    recall  f1-score   support

           0       0.51      0.09      0.16    368149
           1       0.50      0.91      0.65    368949

    accuracy                           0.50    737098
   macro avg       0.51      0.50      0.40    737098
weighted avg       0.51      0.50      0.40    737098
```

(d) Naïve Bayes

```
              precision    recall  f1-score   support

           0       0.99      0.97      0.98    368149
           1       0.97      0.99      0.98    368949

    accuracy                           0.98    737098
   macro avg       0.98      0.98      0.98    737098
weighted avg       0.98      0.98      0.98    737098
```

(e) Stacking Algorithm

Figure 6: Classification Report

Figure 6 (a) shows that the values obtained for precision, recall, and F1-score for random forest as the classifier are 0.86, 0.96, and 0.91, respectively. These values, however, are obtained for class 0, which indicates that legitimate and genuine transactions are taking place. Aside from these, the values obtained for precision, recall, and F1-score for random forest as the classifier look to be 0.96, 0.84, and 0.90, respectively. These numbers, however, are found for class 1, indicating fraudulent transactions.

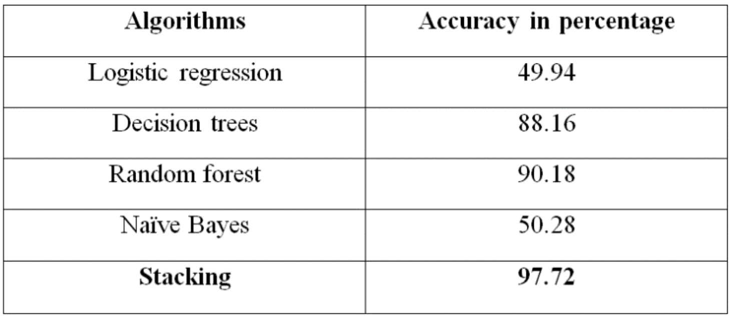
Similarly, decision trees, logistic regression, Nave Bayes, and stacking algorithms can be used to compute the precision factors for legitimate and fraudulent cases.

Conclusions

The primary goal of this paper is to discover credit card fraud cases in the downloaded data file. The thesis will be implemented by automating the process of CCFD detection from the dataset and identifying them as authentic or fake. After this data has been collected, it undergoes pre-processing, which includes duties such as cleansing. Due to the imbalanced and duplicate nature of the data obtained from the repository, the study also presents the SMOTE conceptual theory to balance the dataset. At this stage, the dataset is filtered and cleaned to remove redundant and noisy data. The filtered dataset is then utilised as input for the process of feature engineering, which pulls useful properties from the dataset. The feature engineering process is a critical aspect of the total implementation. The execution of a literature analysis revealed that factors such as gender, state, zip code, employment, and occupation, among others, greatly influenced the probability that scams would occur. Hence, all important elements were considered during the implementation of the thesis. When the characteristics have been extracted, the dataset undergoes the classification phase. This operation is performed so that only a subset of the initially collected features can be given to data mining algorithms. Following the acquisition of a masked dataset, machine learning algorithms are employed to train and evaluate the system model. All unknown and missing variables have been identified, and the training and testing phases have been merged into a single database. It was discovered that labelling each object as "credit card fraud detection" was a significant element of both the train and test versions. This attribute was introduced and applied to target variables to generate a confusion matrix. The dataset must finally be transformed to a numeric datatype because the thesis will use stacking methods; this required altering the object type to a numeric or integer datatype. For the suggested thesis, four machine learning algorithms and one stacking algorithm are utilised, namely;

- Random forest
- Decision trees
- Logistic regression
- Naïve Bayes
- Stacking algorithm

However, the implementation is still in the testing phase and its accuracy is being evaluated further. The accuracy of each of these methods is indicated in the following table:



Algorithms	**Accuracy in percentage**
Logistic regression	49.94
Decision trees	88.16
Random forest	90.18
Naïve Bayes	50.28
Stacking	**97.72**

Table1: List of accuracies

As seen in Table 1, the stacking algorithm produced the highest possible accuracy of 97.72 percent. As a result, the stacking algorithm employing decision tree and logistic regression as the base estimator and random forest as the Meta estimator is selected as the best model.

References

[1] Andrea Dal Pozzolo. Adaptive Machine Learning for Credit Card Fraud Detection. PhD thesis, 2015

[2] M. Ummul Safa and R. M. Ganga. "Credit Card Fraud Detection Using Machine Learning." 2019 International Journal of Research in Engineering, November-2019.

[3] Aderemi O Adewumi and Andronicus A Akinyelu. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8(2):937–953, 2017

[4] Changjun Jiang, et al. "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism." IEEE Internet of Things Journal, 5 (2018), pp. 3637-3647

[5] Analysis and Study on the Classifier Based Data Mining Methods SN Popat, YP Singh Journal of Advances in Science and Technology| Science & Technology 14 (2)

[6] Pumsirirat, A. and Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. International Journal of Advanced Computer Science and Applications, 9(1)

[7] Thennakoon, Anuruddha, et al. Real-time credit card fraud detection using machine learning. In: 2019 9th international conference on cloud computing, data science & engineering (Confluence). IEEE; 2019

[8] Campus K. Credit card fraud detection using machine learning models and collating machine learning models. Int J Pure Appl Math. 2018;118(20):825–38

[9] Varmedja D, Karanovic M, Sladojevic S, Arsenovic M, Anderla A. Credit card fraud detection-machine learning methods. In: 18th international symposium INFOTEH-JAHORINA (INFOTEH); 2019. p. 1-5

[10] Efficient Research on the Relationship Standard Mining Calculations in Data Mining SN Popat, YP Singh Journal of Advances in Science and Technology| Science & Technology 14 (2)

[11] Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: a comparative analysis. In: International conference on computer networks and Information (ICCNI); 2017. p. 1-9

[12] Guo S, Liu Y, Chen R, Sun X, Wang X. X, Improved SMOTE algorithm to deal with imbalanced activity classes in smart homes. Neural Process Lett. 2019;50(2):1503–26