Future Computing and Informatics Journal

Volume 7
Issue 1 (2022) *Issue 1*

Article 2

2022

Credit Card Fraud Detection Using Machine Learning Techniques

Nermin Samy Elhusseny
BIS Helwan University, nerminelhusseny5@gmail.com

shimaa mohamed ouf
BIS helwan university, shimaaouf@yahoo.com

Amira M. Idrees AMI
Future University in EGypt, amira.mohamed@fue.edu.eg

Recommended Citation

Elhusseny, Nermin Samy; ouf, shimaa mohamed; and Idrees, Amira M. AMI (2022) "Credit Card Fraud Detection Using Machine Learning Techniques," *Future Computing and Informatics Journal*: Vol. 7: Iss. 1, Article 2.
DOI: https://doi.org/10.54623/fue.fcij.7.1.2
Available at: https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2

Future Computing and Informatics Journal

Homepage: https://digitalcommons.aaru.edu.jo/fcij/

Doi: http://doi.org/10.54623/fue.fcij.7.1.2

Credit Card Fraud Detection Using Machine Learning Techniques

Nermin Samy Elhusseny[1, a] , Shimaa mohamed ouf [1, b] , Amira M. Idrees [2, c]

[1] Business Information Systems, Faculty of commerce and business administration - Helwan University.

[2] Faculty of Computers and Information Technology, Future University in Egypt.

[a] nerminelhusseny5@gmail.com, [b] shimaaouf@yahoo.com, [c] amira.mohamed@fue.edu.eg

Abstract:

This is a systematic literature review to reflect the previous studies that dealt with credit card fraud detection and highlight the different machine learning techniques to deal with this problem. Credit cards are now widely utilized daily. The globe has just begun to shift toward financial inclusion, with marginalized people being introduced to the financial sector. As a result of the high volume of e-commerce, there has been a significant increase in credit card fraud. One of the most important parts of today's banking sector is fraud detection. Fraud is one of the most serious concerns in terms of monetary losses, not just for financial institutions but also for individuals. as technology and usage patterns evolve, making credit card fraud detection a particularly difficult task. Traditional statistical approaches for identifying credit card fraud take much more time, and the result accuracy cannot be guaranteed. Machine learning algorithms have been widely employed in the detection of credit card fraud. The main goal of this review intends to present the previous research studies accomplished on Credit Card Fraud Detection (CCFD), and how they dealt with this problem by using different machine learning techniques.

Keywords: machine learning, credit card fraud detection, SVM, Random forest, decision tree, naïve Bayes, XG Boost.

1. Introduction:

The payment industry is increasingly offering digital payment methods for a variety of reasons, including time savings, the ability to pay for purchases over time, the expansion of the market, ease of use, convenience, credit card rewards, price protection, purchase protection, and travel benefits, However, it is susceptible to internet fraud and may increase business expenditures. unfortunately, With the current trend of financial inclusion, increasingly offering digital payment methods, and marginalized people being introduced to the financial sector, the number of card users increases, so does the revenue, making them more vulnerable to fraud.

Credit card fraud can take the following forms:

1- Physical card fraud: when a cardholder physically offers his or her card to a merchant in order to complete a purchase. consumer information may be stolen without the customer's knowledge.

2- Virtual card fraud: in online shopping, the password, expiration date, and CVV number are all used. this information can be stolen and used by scammers to carry out fraudulent online transactions.

Figure 1 presented below introduced the credit card fraud detection scenario

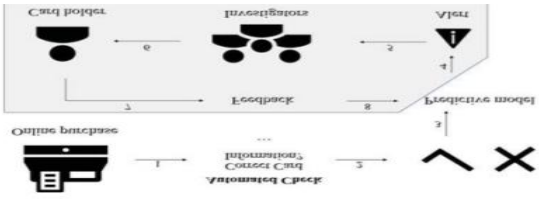

Figure 1: credit card fraud detection scenario [18]

As presented in Figure 1: the credit card fraud scenario: Fraud detection refers to the process of detecting fraud as soon as feasible after it has occurred. Methods for identifying fraud are always evolving to keep up with ever-changing fraud methods. Several technologies, including as statistics, rule engines, artificial intelligence, and data mining, are currently used to detect fraud. Fraud detection occurs at many levels, depending on how long has passed after a particular

Published by Arab Journals Platform, 2022

transaction occurred. The first level, as indicated in Figure 1, is automated card validation, which is done in real time for the benefit of the user. If a card is not denied, the transaction moves to the second level, which is referred to as the predictive model [18].

There has been a surge in interest in using machine learning as a data mining strategy for second-level credit card fraud detection over the last decade. The second level occurs when a certain period of time has passed since the transaction was completed. The automated predictive model, which is part of the second level, detects fraud by looking for anomalies in data and trends. An alarm is raised for the questionable transaction, which necessitates human expert assistance. The shaded area in this diagram only applies to those transactions. Investigators determine whether a transaction is fraudulent or not after evaluating extensive transaction data and, in some situations, contacting the cardholder, and providing comments in order to enhance the accuracy of the prediction model utilized [18].

So, most of financial institutions tended to use intelligence technologies like machine learning, Because of their benefits, whether for the institution or individuals. The classification of credit card fraud detection is based on supervised and unsupervised learning systems. Which were then divided further, into supervised learning systems like AIS, EXPERT SYSTEM, ANN(BP), and others. unsupervised learning has HMM, ANN(SOM), ASI and FUZZY SYSTE, and others.

Researchers can solve the problem of credit card fraud to a good extent by combining these two technologies. Fraudsters typically commit fraud by gaining access to a card's data. To hack it, they don't need an actual card. They can easily conduct transactions using card information. There is no standard approach for stopping it from the root cause, although various methods can be used to identify it. So, by supplying the model with credit card fraud data and using supervised learning to classify the categories of fraud and secrecy, researchers can train the model and predict the outcome of the transaction using the machine learning method.

2. Types of Fraud:

There are three types of financial fraud (Insurance fraud, corporate fraud, and bank fraud), this systematic review focus on the bank fraud type which includes other types like (credit card fraud, mortgage fraud, and money laundering), credit card fraud is the most important type in bank fraud, which takes the most attention, is credit card fraud because of the losses it causes, both to the institution or to individuals. Figure 2 below presented the types of financial fraud while **figure 3:** introduced types of credit card fraud which are divided into two types: Behavioural fraud and application fraud, which will be explained in detail below.

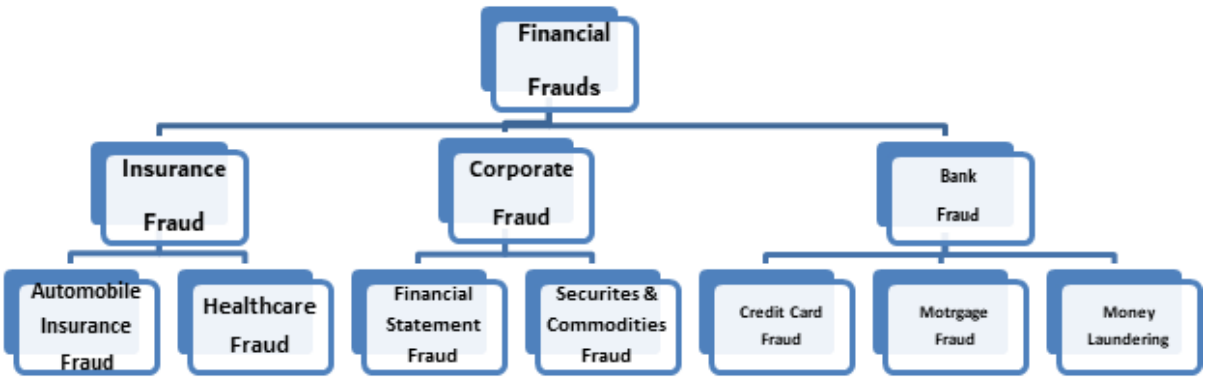

Figure 2: types of financial fraud

2.1. Behavioural Fraud: the first type of credit card fraud is a Behavioural fraud that has four types introduced:

2.1.1. stolen/lost card: criminals steal a credit card to get access to a lost card

2.1.2 mail theft: Before reaching the real user, fraudsters receive credit cards in the mail.

2.1.3. counterfeit: fraudsters take card information from one source and use it on websites that do not require a physical card.

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

2.1.4. merchant collusion and triangulation: Criminals pose as an intermediary site, collecting customer credit card information and redirecting orders using stolen credit card information.

2.2. Application frauds: the second type of credit card fraud is Application fraud which has six types introduced:

2.2.1. Account theft and suspicious transactions: Criminals can utilize personal information such as a Social Security number, a secret question answer, or a date of birth taken from an individual to conduct financial transactions. Because identity theft is linked to a large number of fraud transactions, financial fraud detection systems should focus on establishing an analysis of a user's behavior.

2.2.2. Clone transactions: Among the various kinds of credit card frauds, clone transactions are common. It simply refers to replicating or making transactions that are similar to the original. When an organization tries to collect payment from a partner many times by sending the same invoice to different departments, this can happen.

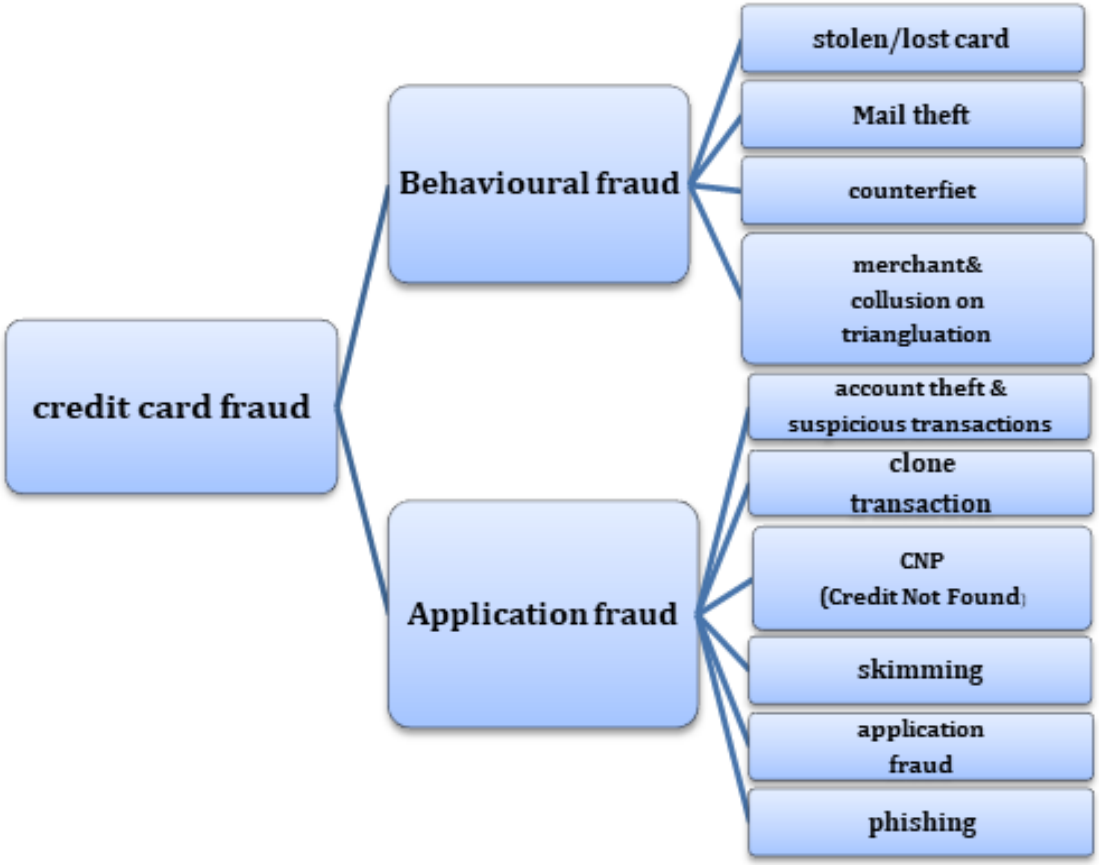

Figure 3: types of credit card fraud

2.2.3. Credit Card Skimming (electronic or manual): Making an illegitimate clone of a credit or bank card with a device that reads and copies information from the original card is known as credit card skimming or credit card forging. Scammers extract card numbers and other credit card information with equipment known as "skimmers," save it and resale it to criminals.

2.2.4. CNP (Card Not Present) Fraud: This could happen if criminals discover the card's expiration date and account number. These two factors are critical when making an internet purchase. More retailers are requiring the verification code these days, but it is not difficult to obtain if you know your account number and expiration date. Criminals can simply try to enter the verification code at a low frequency and eventually figure it out. Anomaly detection tools, such as Machine Learning, may be useful in detecting suspicious trends in a client's activity in order to combat this form of fraud.

2.2.5. Phishing: it is a very common type of data theft method. The victim receives a legitimate-looking email posing as a representative of a well-known organization. It could be a request to update account information or transmit additional personal data in response to "changes" in the organization's policy or for any other cause. The victim transmits their personal information without paying enough

Published by Arab Journals Platform, 2022

attention to the fake domain names, modified logo, or language issues in the content.

2.2.6. False application fraud: It refers to when someone opens a new credit account or credit card in the name of someone else. First, the fraudsters take the documents that would be used to support their false application.

3. Literature Review in Fraud Detection:

All the researchers included in this survey have the same problem that shows: Every day, a large number of credit card transactions are made. As a result, credit card theft has increased, resulting in financial losses for both financial institutions and individuals. Because fraudsters modify their methods all the time, detecting credit card theft is particularly difficult. Traditional procedures are not guaranteed to be accurate and take more time. As a result, the most beneficial machine learning techniques have recently been applied. that assist in automatically detecting fraud, effectively identifying frauds, fast detecting fraud cases streaming, and the ability to detect online fraud in real-time, requiring less time for variation approaches, and identifying hidden correlation data. The purpose of this survey is to examine the most commonly used techniques for identifying credit card fraud and to determine which algorithm produces the best results.

In[1]. This research has included different machine learning algorithms (SVM, Logistic Regression, Naïve Bayes, K-Neighbour classifier, The Random Forest) used to detect credit card frauds and introduced a comparative study between different algorithms.

They run an experiment to see which algorithm is the most effective at detecting credit card fraud. SVM, Nave Bayes, Logistic Regression, KNN, and Random Forest are among the five methods used. The random forest provides the best score result, followed by KNN. The MCC is used to assess an algorithm's performance; its best score is 1 and its values range from -1 to 1. Random Forest gave the closest score of 1 based on MCC measured values, which is 0,848. KNN is 0, 793, Logistic Regression and Nave Bayes are 0,761 and SVM is 0, 558. Then they use the Grid search parameters in the Random Forest algorithm and look for the best results. they observe best score of MCC generated by the Random Forest algorithm IS 0.89.

The result of the SVM algorithm which has True positive is 71073, false negative is 75, false positive is 9, True negative is 45. According to their confusion matrix, the proper predicted values in this model are 71,118, whereas the wrong projected values are 84. The best result for SVC when using the conventional performance measurement score of MCC (Matthews Correlation coefficient) for binary Classification is 0. 558. All other algorithms follow the same procedure, but the approaches are different.

The Logistic Regression model has MCC score of 0.761. where the MCC's best score is 1 compared to MCC's highest score, indicating that it is a better algorithm for detecting credit card fraud. For this dataset, the Naive Bayes algorithm produces the same matrix as Logistic Regression. That means the Nave Bayes algorithm's MCC score for the given dataset is 0.761. where The MCC result of the KNN algorithm for the KNN algorithm is 0.793. The result of the Random Forest algorithm. This algorithm made 71,168 correct predictions and 34 incorrect predictions. Finally, given the above-mentioned parameters, the MCC score of Random Forest is 0.848.

The best MCC score is 0.848, which is obtained using Random Forest with random parameters. Then they used the Random Forest algorithm and used the Grid Search method to identify the best parameters, after which they produced a new model with the new parameters and compared the results. The Random Forest with Grid Search parameters yielded the following results: n estimators = 500, max-features = auto, max depth = 10, criteria = entropy. It has 71071 True positive values, 6 false negative values, 25 False positive values, and 100 True negative values as a result of the confusion matrix. The correct predicted values are 71,171 and the incorrect predictive values are 31. The new resultant algorithm has an MCC score of 0.89.

They discovered that the best value, when compared to MCC's best score, is 1. The Random Forest algorithm generates the closest value, which is 0.89, using new parameters supplied by the Grid search algorithm. They can now deduce that they are achieving greater results as a result of this. They can improve the algorithms by combining them with other algorithms and incorporating new technology into them to get more accurate credit card fraud detection results. This will aid in the reduction of fraud by recognising it early on. Credit card fraudsters will suffer less losses as a result of this.

In[2]. Showed that the most common methods of fraud have been identified in this research. Three classification approaches were utilised to conduct a comprehensive study of credit card history business information in order to develop fraud detection models (Support vector machines, Naive Bayes, and Logistic Regression) and analyze recent findings in this field. and also detailed explanations on how machine learning can be used to improve

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

fraud detection results, including the algorithm, code, explanation tee implementation, and experimentation results.

Precision, recall, F1-measure, and accuracy-based parameters will be used to evaluate the proposed model's performance. They are attempting to increase the accuracy of credit card fraud detection based on the data classification method by employing supervised learning techniques. The results indicate that the SVM kernel is the best algorithm for detecting credit card fraud. Using a ROC graph, the function achieves a 97.2 percent accuracy. While the algorithm achieves over 97.2 percent accuracy, it only achieves 25 percent precision when only a tenth of the data set is considered. When the entire dataset is given into the system, however, the precision increases to 30%. In the event of a fraudulent transaction, the authorized system will be notified, and a response will be delivered to refuse the current transaction. The aim of the algorithm depends on parameters that control how it works. Because the majority of machine learning problems are non-convenes, the model is dependent on the parameters they choose. As a result, the value of parameters may affect the model. They can improve the model by changing these parameters. More algorithms can be added to this model to improve it even further. These algorithms' output, however, must be in the same format as the others. It's simple to add the modules as done in the code.

In[3]. This research presented that to detect fraudulent transactions, the research utilised machine learning techniques such as Artificial Neural Network (ANN), Decision Trees, Support Vector Machines (SVM), Logistic Regression, and Random Forest. Accuracy, Precision, and False alarm rate criteria are used to evaluate the performance of these techniques. They also applied Principal Component Analysis to remove irrelevant from relevant attributes, this leading to select only the desired data such as transaction time, amount, and transaction class, etc.

The strengths and weaknesses of these algorithms were also discussed in this study. It shown that: ANN has the ability to function with incomplete knowledge, stores data on the entire network, fault tolerant, has distributed memory, and can process in parallel. However, it has drawbacks such as being hardware dependent, determining the suitable network structure, network duration being unfamiliar, and network behaviour being inexplicable. It is the strength of the Decision Tree where No feature scaling is required, the technique is resistant to outliers and automatically manages missing values, the training phase takes less time, and it is capable of solving classification and regression problems.

However, it has a drawback. When the amount of the dataset grows larger, a single tree may get more complex, resulting in overfitting. SVM: Effectively suited for structured and semi-structured data, handles high-dimensional data well, and has a low risk of overfitting. However, it has a flaw. Larger datasets take longer to process. Logistic Regression: Its strength is that it is efficient, that it can be over fit in high-dimensional datasets, that it provides improved accuracy, and that it makes no assumptions regarding class scattering in feature space. However, it has a drawback in that it assumes linearity between the dependent and independent variables. Random Forest's strength is that it does not require feature selection, trains the model quickly, and balances the errors.

However, it has a drawback in that it is sensitive to data with a diverse values and attributes with more values. The experiment's data set is sourced from Kaggle. There were 150000 transactions in the obtained dataset. There were a lot of fields in the data collection. They employed Principal Component Analysis to filter irrelevant from relevant variables, resulting in the extraction of only the desired attributes such as transaction time, amount, and transaction class. The True Positive, True Negative, False Positive, and False Negative obtained by machine learning techniques are used to evaluate their performance in detecting fraudulent transactions. The result of the experiment shows that Radom Forest could achieve an accuracy of 99.21%, Decision Tree 98.47%. Logistic Regression 95.55%, SVM 95.16% and ANN 99.92%. The results of the techniques vary depending on the nature and amount of the data set. The ANN model provides accurate results, but it is difficult and expensive to train. SVM works well with little datasets and produces outstanding results. On sampled and pre-processed data, decision tree algorithm performs better, whereas Logistic Regression performs better on raw, not sampled data. For both categorical and continuous data, random forest is an excellent choice.

In [4]. This study presented that compared the performance of two machine learning algorithms in order to determine which one is superior. (Isolation Forest and Local Outlier Factor) They need certain extra standards of correctness to categorise transactions as fraud or non-fraud, such as: F1-score, Support, Precision, and Recall. They introduced Isolation Forest that is a tree-based model for detecting outliers. This algorithm based on the fact that anomalies are rare and distinct data points. Isolation is the outcome of these features, and it is a vulnerable mechanism to anomalies.

This method is fundamentally distinct from all other methods now in use and is extremely beneficial. This algorithm has a low linear time

Published by Arab Journals Platform, 2022

complexity and a small memory requirement. Also, the Local Outlier Factor was introduced, which is used to discover anomalous data points by evaluating the local deviation of a given data point and also respect to its neighbours. This algorithm is used to find outliers based on local density. Locality is determined by nearest neighbours and density calculating by the distance between one can detect regions of similar density and spots that have a significantly lower density than their neighbours by comparing the local density of an object to the local densities of its neighbours.

One can distinguish between regions with similar densities and spots with substantially lower densities than their neighbours. They utilised a dataset were (284807, 31) to train their models, which means it has 284807 training examples. Each training example has 31 features, including Time, Amount, Class, and 28 additional columns labelled V1 to V28. V1 through V28 are the columns that have been modified. PCA transformation is performed for the user's security and to protect the users identify and personal information. PCA transformation is performed for the user's security and to protect the users identify and personal information. The evaluation of metrics to compare performance of models in many classification tasks they used simple evaluation metrics such as Accuracy are used. However, one important disadvantage of accuracy is that it is assumed that each class has an equal representation of examples, which makes accuracy a misleading factor for skewed datasets like ours.

It does not present accurate results. As a result, in their case, accuracy is not an appropriate metric of efficiency. Experimental Results By comparing the results of Local Outlier Factor and Isolation Forest algorithm, showed that the Isolation Forest is superior for detecting the frauds in credit cards. That gave the highest accuracy rate of 97%, and the Local Outlier Factor 76%. Accuracy.

In[5]. The approach proposed in this research employs the most up-to-date machine learning algorithms to detect odd activities known as outliers. The goal of this research is to detect 100% of the fraudulent transactions while cut back the incorrect fraud classifications. They used machine learning algorithms (Local Outlier Factor, Isolation Forest Algorithm, and support vector machine). Their goal is to predict the accuracy/precision of the fraud detection through the different algorithms. This analysis can also be used to implement the fraud detection model. They got the dataset through Kaggle, a site that offers datasets for data analysis. They reduce the amount of data utilised for speedier testing to 10% of the total dataset. When 10% of the dataset is employed, the following results are obtained: isolation forest 99.75 percent accuracy with 71 errors, and local outlier 99.65 percent accuracy with 97 errors. And when use the complete dataset, the following results are obtained:

The accuracy of isolation forest 99.76 percent with 659 errors, the accuracy of local outlier factor 99.67 percent with 935 errors. While the algorithm achieves an accuracy of over 99.6% when just a tenth of the data set is considered, it only achieves a precision of 28% when only a tenth of the data set is considered. But the result with the complete dataset is used the accuracy increased to 33%, the accuracy of Isolation Forest 99.76% with 659 numbers of errors, local outlier 99.61% accuracy and the number of errors was 935, and Support Vector Machine 70% accuracy. As a result, the isolation forest outperforms both the local outlier and the support vector machine

When the entire dataset is given into the algorithm, however, the high percentage of precision has been expected because of the huge imbalance between the number of authentic and number of valid transactions. There were some challenges in this research, it mainly focuses on the analysis of the different Machine Learning algorithms that can detect the credit card fraud with accuracy.

In[6]. Presented this research that considered different machine learning-based classifiers such as random forest, Naive Bayes, XG Boost, logistic regression. for the validation purpose, they have used different metrics such as precision, accuracy, F1, Recall, and MCC of each model but their main focus is on F1 and MCC score. The data sets used in the research were extracted from European Cardholder September 2013, and they reached 284,807 transactions. Only 0.173 percent of the transactions in the overall data set are fraudulent, while the rest are non-fraudulent, indicating that the data sets are extremely imbalanced. As a result, the SMOTE oversampling approach was applied. There are three stages are composed in this experiment. First, the standard model was utilised with the SMOTE technique to deal with the unbalanced data set.

The Random Forest outperformed other techniques with 99.96 percent accuracy, XGBoost 99.95 percent, and Logistic regression 99.93 percent, and Naive Bayes 99.92 percent, according to the results of several individual models. Second, despite the standard model, Soft Voting and AdaBoost, as well as the SMOTE technique, were used with these standard models. The Random Forest + decision tree model outperforms the other models with 99.94 percent accuracy, followed by Naive Bayes + decision tree (99.92 percent), Logistic regression + decision tree (99.91 percent), and XGBoost + decision tree (99.91 percent). As can be seen, the

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

Random Forest + decision tree model has a higher Recall score, while the Naive Bayes + decision tree has a lower Recall and F1 score. Finally, when compared to the standard approach, it can be seen that the rate has decreased.

As a result, the AdaBoost approach is used. It can be shown that, in comparison to other models, the RF model produces the best outcomes. Where random forest accuracy was 99.96%, XGBoost was 99.95%, Logistic regression was 99.93%, and Naive Bayes was 99.92%. The Naive Bayes model shows no change. However, the Random Forest and XGBoost models' Recall, F1, and MCC scores have increased slightly. Furthermore, while the F1 scores of the Logistic Regression and Naive Bayes models do not differ when compared to the individual standard model, it is clear that employing the standard model with AdaBoost improves performance when compared to the other two. Because the score of evaluation measures has risen slightly. in the future this research recommended that the various machine learning models utilised can be extended to deep learning models. In addition, for better outcomes, and the other methods for feature selection and dealing with the problem of data set imbalance can be applied.

In[7]. Showed Six different machine learning models were utilised in this research to assess their performance on a dataset containing real-world transaction data. They look at how well the performance of Random Forest (RF), Support Vector Machine, K-Nearest Neighbour (KNN), Logistic Regression(LR), Classification And Regression Trees (CART), XGBoost, Linear Discriminant Analysis(LDA) for detecting the fraud of credit card. The suggested system displays results based on the precision, sensitivity, specificity, and accuracy. The dataset was used about European cardholders. This dataset shows that, the transactions are made on2013 in two days of September month. it was containing 284,807 transactions. The positive class (fraud cases) make up 0.172 percentage of the transactions data. By using Exploratory Data Analysis, they exploit amount and time. These are the specified identifiers of transactions.

There are four basic metrics for evaluating these kinds of experiments. True positive rate (TPR), True Negative rate (TNR), False positive rate (FPR), and False negative rate (FNR). according to the results, Random forest outperforms XGBoost98.4%, logistic regression 97.7%, Support Vector Machine97.5 percent, Linear Discriminant Analysis97.4%, KNN96.9%, and CART 58.6% Analysing the research's results, it's clear that the obvious result for accuracy is extremely high. However, this does not imply that it will run on every dataset and identify illegitimate ones. For a major part of the research, it was critical that they perfectly extract the dataset's features. Their future work will focus on overcoming this challenge using a genetic algorithm, as well as thorough feature selection and methods that allow for stacked classifiers.

In[8]. The research's goals are to use machine learning for credit card fraud detection, in terms of transaction time and amount. This research trying to build the model that predict fraud and non-fraud transaction in the best way using the machine learning algorithms and neural networks. (Logistic regression, naive Bayes, decision tree, Artificial neural networks (ANN)). The result of classification report for each algorithm, with class 0 indicating that the transaction was considered to be valid and 1 indicating that it was determined to be a fraud transaction.

The transactions from Europe cardholders in September 2013 are included in this dataset. There are 492 fraud transactions out of 2,84,807 totals, because there are fewer fraud cases than there are transactions, the data is unbalanced, and they used oversampling to convert the imbalanced dataset to balanced. The data set has been converted to a PCA transformation and including only numeric values.

Due to privacy and confidentiality concerns, numerous background details are hidden, and given only PCA transformed data. Only time and amount are not transformed to PCA; all other given values (v1, v2, v3, v4, v5, v6, v7, v8, etc.) are PCA transformed numeric values. The fraud feature class has a value of 1 and the normal transaction has a value of 0. They have a 98.69 percent accuracy rate. ANN outperformed all other algorithms, scoring 94.84 percent for logistic regression, 92.88 percent for decision trees, and 91.62 percent for naive Bayes. They employed a confusion matrix to visualise the results in a form table, and all algorithms have a low false positive rate, which is essential to meet the objectives. Finally, utilising basic user interface design, fraud or non-fraud is determined using numerical data.

In[9]. This research using machine learning techniques (Random Forest, Decision Tree, Support Vector Machine). For detecting fraud in Credit Card. They selected features from their transaction dataset using a PCA algorithm, which employs correlation and variance as parameters to choose features. They used the PCA approach to identify the features and set the summation of variance at 95%. They also used the PCA feature selection technique because no features with a high variance and correlation with the class column that determines whether a transaction is fraudulent or not normal transaction. They used a dataset

Published by Arab Journals Platform, 2022

provided by Kaggle, which contains the transaction records of European cardholders from the year 2013. There are 31 columns in the dataset, 30 of which are utilised as features, and 1 column is used as a class. Time, Amount, and Number of Transactions are some of their features. They used the three machine learning methods described in the approach, and the models show that each of them has a high accuracy score. The support vector machine, decision tree, and random forest classifier methods each received 99.8%, 99.7%, and 99.7%, respectively. Because these models have high accuracy but poor precision in their predicted values, they will be working on improving their model in the near future to get the best outcomes with high precision in determining fraud detections in credit card transaction data.

In[10]. this research applied supervised machine learning algorithms On an unique and single dataset, (Decision Tree, Random Forest, K-Nearest Neighbour, Support Vector Machine) on transactions that had previously been identified as fraudulent or not. The goal was to verify the outcomes of their prior state of the art by comparing the strategies that produced the best results on the same dataset. This research is based on a produced dataset with around 60.000 transactions across 12 features. Transaction and client information are examples of these features. For their experience, the dataset has a highly skewed data set, with 99.72 percent of transactions falling into the non-fraudulent category. This is done to get as close to a real financial dataset as feasible, and to imitate real transaction situations.

The MSE of each approach was calculated after using machine learning techniques (MSE training dataset, MSE test dataset), with SVM having the best MSE values (0.0021-0.0024), Random Forest 0.0026-0.0028, K-Nearest Neighbour 0.0028-0.0029, and Decision Tree 0.0027-0.0031. The results showed that the support vector machine outperformed the K-Nearest Neighbour 97.1 percent, Random Forest 82.5%, and Decision Tree 78.9% in terms of accuracy. In terms of accuracy and MSE, it is evident that SVM produces the best results. It is conceivable to investigate the application of neural networks, as well as other supervised, unsupervised, and reinforcement learning techniques, in the future of this research. Their major goal is to figure out which techniques produce the greatest results so that they can incorporate them into their adaptive credit card fraud detection model.

In[11]. This research discusses the supervised based classification by using Bayesian network classifier (K2), Tree Augmented Naïve Bayes (TAN), and Naïve Bayes, logistics and J48 classifiers. The experiments in this research were conducted using two datasets. Data transformation and data reduction were used to create the raw dataset and the new dataset. And TPR, FPR, precision, recall, F-Measure, and accuracy were the measures utilized in this research. They conduct two experiment. The raw dummy dataset was utilised in Experiment 1 to assess the data's integrity for credit card fraud detection. The results showed that TAN had the highest TPR (75.0 percent), precision (73.0 percent), recall (75.00 percent), F-Measure (68.5 percent), and accuracy (84.0 percent) among the classifiers. For the J48, which also was similar based on a tree model showed these results where: TPR (73.0 percent), accuracy (69.4 percent), recall (67.5 percent), and F-Measure (67.4 percent) were somewhat lower than TAN Furthermore, J48's processing speed was slower than TAN's, despite the fact that the latter classifier's operations were heavier and more expensive.

The results of K2 showed that: TPR (31.0%), precision (21.0%), recall (32.0%), F-Measure (32.2%), and accuracy (41.8 %). In experiment 2, the raw dummy dataset was fed into the data transformation and data reduction techniques. The data that had been filtered with normalisation and Principal Component Analysis was used in the second experiment. In comparison to Experiment 1, all five classifiers produced improved outcomes. All of the classifiers were more accurate than 95.0 percent and speed of processing than Experiment 1. J48 and Logistics findings revealed that both classifiers performed.

When compared to the previous experiment, K2 has shown a significant improvement in classification. After the data transformation and data reduction operation, the classifiers increased TPR by over 195.80%. In addition to the TPR, precision, recall, F-Measure, and accuracy improvements, all of the classifiers' processing speeds improved dramatically when compared to the previous experiment. After performing data pre-processing tasks, the performance of the classifiers on the pre-processed dataset is better than the raw dataset, proving the hypothesis of experiment 2. This research will aim to investigate more credit card fraud detections using real-time data in the future.

In [12] To train the behaviour features of legal and illegal transactions, two types of random forests are employed in this research: random tree-based random forest and CART-based-Random Forest. In their experiments, this research also uses alternative algorithms including support vector machines, Naive Bayes, and neural networks. Accuracy, Precision, Recall, F-Measure, Transaction Intervention Rate, and Customer Covered Rate were utilised to measure performance

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

in this research. The research's dataset comes from a Chinese e-commerce company and includes fraudulent and legitimate B2C transactions from November 2016 to January 2017. There are over 30,000,000 separate transactions in the original dataset. There are 62 attribute values in each transaction record. Only around 82,000 transactions were identified as fraudulent in the dataset, implying a fraud ratio of 0.27 percent and must take into consideration the dataset imbalance problem.

Researchers compare the two random forests, which differ in their basis classifiers, and examine their performance in detecting credit fraud. The capacity of a random forest is determined by two factors: the strength of individual trees and the correlation between them. As a result, the better performance of random forest, the stronger the strength of single tree and the less the correlation of different trees, where Random forest is robust to outlier and noisy. They performed three experiments to determine which type of random forest is best for detecting fraud. In addition to support vector machines, naive Bayes, and neural networks, they use various techniques in their research. However, the results are worse than a random forest. CART-based-random forest was shown to be effective in the first experiment. Although the precision is slightly lower, the accuracy, recall, and F-measure are significantly higher. Clearly, the CART-based-random forest's comprehensive performance is far more acceptable for use on this experiment subset. Where R random forest. 0.7811F-Measure, 91.96 percent accuracy, 90.27 percent precision, 67.89 percent recall, Random forest based on CART (Random Forest II) 0.9601 F-Measure, 96.77 percent accuracy, 89.46 percent precision, 95.27 percent recall. The following is the second experiment.

The relationship between a model's performance and the ratio of legitimate and fraudulent transactions is investigated in this experiment. All transactions that have been flagged as fraudulent are kept as the foundation for regulating the under-sampling ratio. The ratio of legitimate to fraud transactions is varied from 1:1 to 10:1 in ten subsets. It is more realistic to consider random forest II. To demonstrate fraud detection effectiveness, the third experiment uses random forest II with a larger and more closely related to the actual application dataset. The training set is derived from the original November and December 2016 dataset. Similarly, all fraud transactions are used in experiment I, while legal transactions are randomly picked to provide a 5:1 ratio of legal to fraud transactions, which has been shown to be the optimal ratio for random forest II. With a 98.67 percent accuracy rate, 32.68 percent precision, 59.62 percent recall, 1.48 percent transaction intervention rate, and 34.09 percent customer coverage rate. They recommended that in the future work have to focus to solve imbalanced data problem, in their future work they will try to make some improvement for the Random Forest algorithm.

In[13]. On extremely skewed data on credit card fraud, this research used machine learning techniques such as support victor machine, Naive Bayes, Logistic Regression, and K-Nearest Neighbour. Validation and testing are carried out on 80% of the dataset. Accuracy, sensitivity, precision, and specificity are used to evaluate these techniques. TPR, TNR, FPR, and FNR were the four metrics utilised to evaluate them. This research used two ways to evaluate the machine learning models: classification accuracy and confusion matrix. The used dataset is from Kaggle. In a CSV file, this dataset contains 3075 transactions with 12 transaction features. Researchers used two distinct methods to evaluate these machine learning models: (Classification accuracy, Confusion Matrix).

The results demonstrate that logistic regression has a high accuracy of 99.074 percent and 98.92 percent specificity, 93.61 percent precision, and 1% sensitivity. Support vector machine (SVM) has 97.53 percent accuracy, 97.56 percent sensitivity, 97.53 percent specificity, and 85.1 percent precision. Where k-nearest neighbour 96.91 percent accuracy, 89.36% sensitivity, 98.19 percent specificity, and 89.36% precision, and Naïve Bayes showed 95.99 percent accuracy, 0 percent sensitivity, 1% specificity, and 1% precision. Across all of the assessment metrics employed, logistic regression yielded the most accurate results. It was more accurate in detecting credit card theft when tested under realistic conditions. Work may require even more processing power in the future. Different bias-avoidance tactics, such as different resampling methods, cost-sensitive learning methods, and ensemble learning techniques, could also be tested in future datasets to determine the optimum strategy for dealing with a skewed dataset.

In[14]. On the original and SMOTE datasets, this research evaluates a few models (local outlier factor-isolation forest-support vector machine-logistic regression-decision tree-random forest). The results reveal significant disparities in accuracy, precision, and MCC. Even one-class SVM was utilised, which is ideal for binary class datasets. They can also utilise on-class SVM because their dataset has two classes. The dataset contains transactions completed by a cardholder over the course of two days in September 2013. There are a total of 284,807 transactions, of which

492 are fraudulent, accounting for 0.172 percent of all transactions. The results indicated that random forest techniques outperform either before or after applying SMOTE, however the results after SMOTE are better than before SMOTE. Which: Before applying:

1-Before using: Local Outlier factor (accuracy: 89.90%) 0.38 percent precision MCC = 0.0172

2-Isolation forest accuracy is 90.11 percent with 1.47 percent precision. MCC = 0.1047

3-support vector machine 99.87 percent precision 0.5257 MCC with 76.81 percent precision

4-Logistic regression has a precision of 87.5 percent and an accuracy of 99.90 percent. MCC = 0.6766

5-Decision tree precision is 88.54 percent and accuracy is 99.94 percent. MCC = 0.8356

6-Random forest has a precision of 93.10 percent and an accuracy of 99.94 percent (0.8268 MCC).

After applying SMOTE:

1-local outlier factor has 45.82 percent accuracy, 29.41 percent precision MCC = 0.1376

2-Isolation forest has 0.2961 MCC 58.83 percent accuracy 94.47 percent precision

3-Logistic regression has 0.9438 MCC 97.18 percent accuracy 98.31 percent precision

4-for the decision tree 97.08 percent accuracy and 98.14 percent precision, and 00.9420 MCC

5-Random forest has a precision of 99.96 percent and an accuracy of 99.98 percent. And 00.9996 MCC. Future study could look into meta-classifiers and meta-learning techniques for dealing with severely skewed credit card fraud data. Other sampling procedures and their impacts can also be examined.

In [15]. This research assessed the performance of various machine learning methods (logistic regression, decision tree, and extreme gradient boosting to detect credit card fraud) on both balanced and unbalanced data, as well as analysed the classification problem with imbalanced data. The accuracy and AUC were used to evaluate performance in this research. Credit card transactions that occurred over the course of two days are included in the dataset used in this research. The data is significantly skewed, with 492 frauds out of 284,807 transactions, or 0.17 percent of all transactions. This study employed approaches to deal with skewed data, and it is commonly used to transform a skewed dataset into a balanced dataset in the following ways: -

• Over-Sampling vs. Under-Sampling• Using KNN to create synthetic data• Cost-Sensitive Learning

The results showed that Logistic regression achieved the highest area under the curve (AUC) where (0.9375) with accuracy of 99.75 percent which is trained on under-sampled balanced data.

The results presented that combining machine learning techniques improves fraud detection performance and accuracy, and the model is 100 percent effective in predicting fraud. Observations after Under sampling revealed that logistic regression had 99.87 percent accuracy, 0.819 percent Area Under the Curve; Observations after Oversampling revealed that logistic regression had 99.1 percent accuracy,.933 percent Area Under the Curve; and Observations after Generating Synthetic Data revealed that logistic regression had 99.857 percent accuracy, 0.9321 percent Area Under the Curve. Finally, the greatest results were seen by under sampling logistic regression with 99.75 percent accuracy and 0.9375 Area Under the *Curve (AUC).*

As a result, anyone can use a credit card, and the company will immediately receive all of the essential logs, which will be utilised in their training dataset, and will test the new entry against their model. - If the result is negative, the credit card is authentic. - If the result is negative, the credit card has been used fraudulently. Their models are effective, and they can anticipate with near-perfect accuracy. This can assist the organisation in protecting their users from making unaware purchases.

In [16]. On highly skewed credit card fraud data, this research study explores and compares the performance of Decision Tree, Random Forest, Support Victor Machine, and logistic regression. And they employed accuracy, sensitivity, specificity, and precision to assess performance. They use 30 input attributes for 284,786 transactions sourced from European cardholders.

The results showed that the Random Forest is outperformance with 98.6% accuracy, 98.4%sensitivity, 90.5%specificity, and 99.7%precision. Decision Tree 95.5% accuracy, 95.5% sensitivity, 87.8% specificity, 99.5% precision. Logistic Regression 97.7% accuracy, 97.5% sensitivity, 93.2% specificity, 99.6% precision. Support Vector Machine 97.5% accuracy, 97.3% sensitivity, 91.2% specificity, 99.6% precision. With more training data, the Random forest algorithm will perform better, but speed during testing and application will decrease.

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

More pre-processing techniques would also be useful. The SVM algorithm still suffers from the imbalanced dataset problem and requires more pre-processing to produce better results. While the results produced by SVM are excellent, it could have been much better if the data had been pre-processed on the data.

In [17] this research used decision trees, K-Nearest Neighbour Algorithm, logistic regression, and neural networks to construct fraud detection models. The confusion matrix, sensitivity, specificity, false positive rate, balanced classification rate, and Matthew's correlation coefficient are some of the performance measures that could be used to report the fraud detection classifiers' performance. The data set contains real-life data from an e-commerce organization. There are 1,000,000 records in the dataset, with 9 attributes. In the process of training and testing the different models, this research used 0-fold, 5-fold, 10-fold, 15-fold, and 20-fold cross validation to avoid bias, the average results of each algorithms showed that: the logistic regression is outperforming with 96.27% accuracy, 96.85% sensitivity, 81.39 % specificity. Where KNN 95.85% accuracy, 96,66% sensitivity, 74.93% specificity, Decision Tree 94.366% accuracy, 94.67% sensitivity, 72.2% specificity, and Neural Network 88.39% accuracy, 97.14% sensitivity 58.70% specificity.

The results indicate that logistic regression-based approaches outperform with the highest accuracy, and it may be employed effectively by fraud investigators. Developing a fraud detection model employing a combination of different data mining methods (ensemble) could help improve performance.

In [18]. In this research, researchers assess the performance of three machine learning algorithms in identifying fraud on real-world data including credit card transactions: random forest, support vector machine, and logistic regression. They used a real-life, extremely imbalanced dataset created by European cardholders in September 2013 over the course of two days with 284807 transactions. For an imbalanced dataset, they adopted the SMOTE approach. Precision, recall, and FPR are three regularly used metrics for evaluating technique performance.

They use three learning approaches: static learning (the AUC for three algorithms is similar performance, and random forest is the best), and the accuracy results were: Random Forest 84.83%, support vector machine 79.78%, and logistic regression 73.37%. The second approach was incremental learning (the three algorithms are similar in performance, but the support vector machine is better when precision is used, and SVM and LR are better in this approach), and the accuracy results were: random forest 82.93%, support vector machine 80.36%, and logistic regression 84.13%. the third approach was periodic re-training (more resistant to nonstandard input items). They investigate the performance of three machine learning algorithms that were chosen based on past research and are similar to the most often used Machine Learning techniques in CCFD. They also employ oversampling techniques to handle the problem of unbalanced classes.

Random forest performs better in static (as assessed by AUC), whereas SVM and Logistic regression perform better in incremental, with the latter having much better outcomes than its static version. In terms of both static and incremental learning, a comparison of all three methods measured using AP (plotted as precision-recall curve). Because the curves overlap, it's impossible to say one algorithm is considerably superior to the others. Random forest and SVM perform similarly. While for the higher recall values logistic regression comes closer to random forest and SVM decrease in performance. In the future work they Work on producing real-life data.-

In [19]. This research suggested a system for fraud detection that consists of two components.

1-Designing a data-pre-processing framework: The system is primarily comprised of a Hadoop network that stores data in HDFS that comes from many sources. SAS reads Hadoop data and converts it to a raw data file using the data step and proc Hadoop step. A delimiter is used to separate the fields in a raw data file. The analytical model receives the raw data file in order to construct the data model. This makes the system very scalable and aids in the development of a strong self-learning analytical model in real time.

2- Designing a fraud prediction analytical model: The analytical model is utilised to determine whether or not the incoming transaction is genuine or not. The logistic regression and decision tree and Random Forest Decision Tree models were employed to solve the regression and classification problems, respectively. These models are used to detect fraud using a confusion matrix, which explains how the tuples in the training and testing models are classified correctly. The three models run on the dataset of credit card. And with help of confusion matrix, the accuracy of analytical model is evaluated. They also used F1SCORE, specificity, sensitivity, and precision.

The results showed that random forest is better than others with 76% accuracy, 77% recall, 69% specificity, and 93% precision, 61% f1 score. And

come after it Decision tree with 72% accuracy, 75% recall, 56% specificity, 89% precision, 71% f1 score. And logistic regression with 72% accuracy, 88% racall, 36% specificity, 76% precision, f1score 70% The only issue with random forest is overfitting of the tree in memory as data increases. The goal of this research in the future is to solve the decision tree overfitting problem and detect real-time fraud transactions for high-streaming real-time data.

In [20]. This research showed that to predict the outcome of regular and fraudulent transactions, it employs (naive Bayes, C4.5 decision tree, and bagging ensemble machine learning techniques). Precision, recall, and PRC area rates are used to assess algorithm performance. Machine learning techniques have PRC rates between 0.999 to 1,000, indicating that they are quite good at discriminating binary class 0 in given dataset. The dataset covers credit card transactions done by European cardholders in September 2013. There are 284.807 transactions in this dataset, with 492 of them being fraudulent.

They compare the performance of Naive Bayes, C4.5 decision tree machine, and bagging ensemble methods using recall, precision, and precision-recall curve (PRC) area rates in this research. Bagging with C4.5 decision tree as base learner has the best PRC class 1 rate of all algorithms, with a rate of 0,825. The C4.5 decision tree algorithm was used to forecast fraud transactions with a success rate of 92,74 percent. PRC Area rates for the 0 class are between 0,999 and 1,000 as a consequence of the performance of machine learning methods, indicating that these algorithms are highly good at differentiating binary class 0 in our dataset. PRC rates for class 1 results are 0,080 for naive Bayes, 0,745 for C4.5 decision tree, and 0,825 for bagging ensemble learner, indicating that naive Bayes algorithms perform poorly, whereas C4.5 and bagging are effective in differentiating binary class 1.

This is a significant indicator because we were testing algorithms to determine whether a transaction was normal or fraudulent. When they talk about the precision rate of class 1, they're referring to the negative predicted value or the accuracy of the class 1 alarm rate. As a result of the best performing C4.5 decision tree algorithm, 92,74 percent of all predicted fraud transactions would be correctly forecasted.

The confusion matrix summarises the algorithm's performance. Where class 0 mean positive, and class 1 mean negative. The results of class 0 were: Naïve Bayes 99.9% precision, 97.8% recall, 1.000 PRC area, C4.5 was 1.000 precision, 1.000 recall. .999 PRC area, and bagging was 1.000 precision, 1.000 recall, 1.000 PRC area.

Overall, the highest performing algorithm, according to the PRC Area, is bagging with C4.5 decision tree as base learner, with a rate of 1,000 for class 0 and 0,825 for class 1. In the performance of the naive Bayes model has the highest recall rates of 0,978 for class 0 and 0,829 for class 1 are recorded. In the performance of the C4.5 decision tree model, the highest precision rates of 1,000 for class 0 and 0,927 for class 1 are recorded.

In [21]. This research depended on a slightly skewed credit card fraud data set, this research assessed the performance of various techniques (random forest, tree classifiers, artificial neural networks, support vector machine, Nave Bayes, logistic regression, and gradient boosting classifier strategies). Precision, recall, F1-score, accuracy, and FPR % have all been used to evaluate the efficacy of different techniques.

The research acquired data from European cardholders for the deployment of the machine learning approach for credit card data set, which mostly contains transactional data through credit card emerges with a total of 284,807 transactions. Precision, recall, F1-score, accuracy, and FPR % have all been used to evaluate the efficacy of different techniques. Greater values have been proved to be accepted as just a higher performance method of precision, accuracy, recall, and F1-score for any machine learning technique. The percentage of the different assessment parameters for just the credit card fraud dataset for various machine learning techniques is shown in the experimental outcomes. The results show that random forest techniques outperform other techniques in terms of accuracy, precision, recall, f1-score, FPR, and % accuracy with 94.9991%, 95.9887%, 95.1234, 95.1102, 3.9875

KNN
94.999 %, 94.5891%, 92.008%, 91.003% ,91.7752%, 3.998

GBM
94.001%, 93.998%, 93.001%, 93.998%, 93.556%, 4.665,

SVM
93.963%, 93.228% 93.005%, 93.479%, 92.789%. 3.889,

NB
91.8887%, 91.201%, 91.989%, 91,7748%, 91.0021%, 4.7789,

DT

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

90.998%, 90.998%, 91.996%, 92.778%, 91.7753%, 4.665,

LR
90.448%, 92.8956%, 93.112%, 92.112%, 91.5456%, 3.9785.

There are a few algorithms that have greatly outperformed others. As a result, choosing Random Forest over all other techniques could be a valid approach for achieving a higher degree of completeness while reducing quality only noticeably. In the future, the proposed method might be implemented and tested on vast amounts of real-time data using a variety of machine learning algorithms.

In [22]. This research presented the performance of three unsupervised machine learning techniques (Local Outlier Factor, Isolation Forest Algorithm, and K-means clustering) on imbalanced credit card fraud data is evaluated in this research. They assessed the algorithms using accuracy, sensitivity, specificity, PR-AUC, Matthews's correlation coefficient, and balanced classification rate as evaluation metrics. The experiments that ran on the dataset were split into two sections or components. The first phase entails dividing the dataset into three different ratios:

1. 60 percent training set, 40 percent testing set (the accuracy of Isolation Forest was 99.7787 percent Local Outlier Factor 99.6752 Percent K-Means Clustering 53.9978 percent)
2. 70 percent training set, 30 percent testing set (the accuracy of Isolation Forest was 99.7799 percent, Local Outlier Factor 99.6804 percent , K-Means Clustering 53.8756 percent)
3. 80 percent training set, 20 percent testing set (the accuracy of Isolation Forest was 99.7928percent, Local Outlier Factor 99.6804 percent, K-Means Clustering 53.9043 percent)

The results shows that Isolation forest outperforms the other two algorithms in overall performance evaluation.

The accuracy of the local outlier factor and isolation forest algorithms are equivalent in the experiment, but isolation forest exceeds local outlier factor by a very close margin, and k-means clustering is lacks in its accuracy and also has the lowest accuracy. They tested whether the imbalance dataset classification methods, which include oversampling and under sampling, improve algorithm performance in the second phase.

In this phase, they've also covered a crucial topic: hyper parameter setting for algorithms, which entails setting hyper parameters in algorithms to maximise their performance for datasets with class imbalance problems. To assess the evaluation of their machine learning models, they used K-fold cross validation. In all of the metrics studied, the Isolation Forest outperforms both the Local Outlier Factor and K- mean clustering, according to the results of the experiment. Meta-classifiers and meta-learning approaches for handling with highly imbalanced credit card fraud data may be investigated in the future. It is possible to investigate the usage of ensemble methods and the combination of various algorithms into modules. They'll create a Big Data-driven ecosystem and put their system to the test using a larger and variety of datasets.

In [23]. Researchers have observed a variety of machine learning methods; however, Auto Machine Learning is yet to be discovered on a larger platform. As a result, the initial goal of this research is to investigate the popular Auto Machine Learning technology.

Which were then compared to Machine Learning and Auto Machine Learning. (Pre-processing, Oversampling, Splitting the dataset into test and train data, Feature Selection, AUTO ML (This is the key portion of the complete model.)) Was their proposed model. (Extra trees, Random forest, linear discriminant analysis, ada boost, logistic regression, decision tree, ridge classifier, gradient boosting, KNN, SVM-Linear kemel, light gradient boosting, Naive Bayes, quadratic discriminant analysis) are among the thirteen algorithms used to evaluate the described model. On a variety of metrics such as accuracy, f-1 score, recall, time, and precision.

The table 1 below presented the all the techniques results used that obtained in the previous research while table 2 below presented the source and size of dataset in previous researches.

REF.	Techniques	Acc.	Recall	Sensitivity	Specificity	Precision	MCC	F1	AUC
[1]	RF KNN LR NB SVM		*0.90* *0.84* *0.83* *0.91* *0.92*				*0.848* *0.793* *0.761* *0.761* *0.558*	*1.00* *1.00* *1.00* *0.98* *1.00*	

[2]	SVM Kernel NB LR	*97.2%*				*30%*			
[3]	ANN RF DT LR SVM	*99.92%* *99.21%* *98.47%* *95.55%* *95.16%*				99.57% 92.34% 84.98% 83.76% 88.42%			
[4]	*Isolation forest* *Local Outlier Factor*	*97%* *76%*	*1.00* *1.00*			*1.00* *1.00*		*1.00* *1.00*	
[5]	*Isolation forest* *Local outlier* *SVM*	*99.75%* *99.65%* *70%*							
[6]	 *RF* *XGBoost* *LR* *NB* *RF+DT* *NB+DT* *LR+DT* *XGBoost+ DT* *RF* *XGBoost* *LR* *NB*	Individual models *99.96%,* *99.95%* *99.93%* *99.92%* Soft voting *99.94%* *99.92%* *99.91%* *99.91%* AdaBOOST *99.96%* *99.95%* *99.93%* *99.92%*	Individual models *0.83* *0.83* *0.68* *0.66* Soft voting *0.80* *0.80* *0.80* *0.80* adaboost *0.84 0.83 0.69 0.66*			Individual models *0.95* *0.92* *0.91* *0.86* Soft voting *0.88* *0.76* *0.74* *0.72* AdaBOOST *0.95* *0.92* *0.90* *0.86*	Individual models *0.8900* *0.8726* *0.7876* *0.7497* Soft voting *0.8416* *0.7802* *0.7729* *0.7592* adabost *0.8975* *0.8764* *0.7884* *0.7497*	Individual models *0.89* *0.87* *0.78* *0.74* Soft voting *0.84* *0.78* *0.77* *0.76* adaBOST *0.90* *0.88* *0.78* *0.74*	
[7]	*RF* *XGB* *LR* *SVM* *LDA* *KNN* *CART*	*98.6%* *98.4%* *97.7%* *97.5%* *97.4%* *96,9%* *58.6%*		*0.984* *0.983* *0.975* *0.973* *0.955* *0.937* *0.885*	*0.905* *0.9010.923* *0.912* *0.878* *0.971* *0.91*	*0.997* *0.994* *0.996* *0.996* *0.995* *0.991* *0.94*			
[8]	*ANN* *LR* *DT* *NB*	*98.69%* *94.84%* *92.88%* *91.62%*	*98.98* *92.00* *86.34* *84.82*			*98.41* *97.58* *99.48* *97.09*			
[9]	*SVM* *RF* *DT*	*99.8%* *99.7%* *99.7%*							
[10]	*SVM* *KNN* *RF*	*99.7%* *97.1%* *82,5% 78,9%*							

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

	DT								
[11]	J48 LR TAN NB K2	100% 100% 99.7% 96.7% 95.8%				100.0% 100.0% 98.4% 95.6% 92.6%			
[12]	CART-based-RF RF	96.77% 91.96%	67.89% 95.27%			89.46% 90.27%			
[13]	LR SVM KNN NB	99.074% *97.53%* *96.91%* *95.99%*		1% *97.56%* *89.36%* 0%	98.92% *97.53%* *98.19%* 1%	93.61% *85.1%* *89.36%* 1%			
[14]	RF DT LR IF Local Outlier	99.98% 97.08% 97.18% 58.83% 45.82%				99.96% 98.14% 98.31% 94.47% 29.41%	99.96% 94.20% 94.38% 29.61% 13.76%		
[15]	 LR DT EXG Boostig LR DT EXG Boostig LR DT EXG Boostig	observations 99.87% 99.92837 99.95% after Undersampling 99.75% 99.21% 98.8% after Oversampling 99.1% 98.45% 99.92% after Generating Synthetic Data: 99.857% 82.79% 99.75%							Observations: 0.819 0.8215 0.886 after Undersampling: 0.9375 0.9341 0.9319 After Oversampling: 0.933 0.933 0.912 after Generating Synthetic Data: 0.9321 0.9321 0.9269
[16]	RF DT SVM LR	98.6% 95.5% 97.5% 97.7%		98.4% 95.5% 97.3% 97.5%	90.5% 87.8% 91.2% 92.3%	99.7% 99.5% 99.6% 99.6%			
[17]	LR KNN DT NN	96.27% 95.85% 94.366% 88.39%		96.85% 96.66% 94.67% 97.14%	81.39% 74.93% 72.2% 58.70%				
[18]	 RF SVM LR								Static learning: 91.48% 88.77% 91.13% Incremental learning: 90.13% 86.78% 91.07%

[19]	RFDT DT LR	76% 72% 72%		77% 75% 88%	69% 56% 36%	93% 89% 76%		61% 71% 70%	
[20]	C4.5D NB Bagging		1.000 0.978 1.000			1.000 0.999 1,000			
[21]	RF KNN GBM SVM NB DT LR	94.99% 94.99% 94% 93.96% 91.88% 90.99% 90.44%	95.1234% 92.008% 93.001% 93.005% 91.989% 91.996% 93.112%			95.9887% 94.5891% 93.998%93. 228% 91.201% 90.998% 92.8956%		95.11 91 93.99 93.47 91.77 92.77 91.11	
[22]	Isolation forest Local Outlier K-Means	99.7787%- 99.7799%- 99.7928% 99.6752%- 99.6804&- 99.6804% 53.9978%- 53.8756%- 53.9043%		0.998927 - 0.998862 - 0.998927 % 0.998320 - 0.998323 - 0.998294 % 0.54- 0.538- 0.539%					
[23]	ET RF IDA ADA LR DT RIDGE GBC KNN SVM Lightbm NB QDA	99.96% 99.95% 99.93% 99.92% 99.91% 99.91% 99.89% 99.89% 99.84% 99.82% 99.51% 99.26% 97.58%	79% 78% 73% 70% 60% 75% 42% 41% 5% 0% 53% 62% 86%			94.6% 94% 85% 82% 81% 74% 82% 77% 81% 0% 21% 13% 5%	86% 85% 79% 75% 69% 74% 58% 54% 21% - .0002% 33% 29% 22%	86% 85% 78% 75% 69% 74% 55% 50% 10% 0% 295 22% 10%	94% 94% 90% 97% 94% 87% 0% 56% 60% 0% 69% 96% 96%

Table 1: the results of techniques

:

Ref.	Dataset source	Dataset size
[1]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[2]	**Not mentioned**	**Not mentioned**
[3]	**Kaggle**	**150000 Transactions**
[4]	**Kaggle**	**284807 transactions**
[5]	**Kaggle**	**Not mentioned**
[6]	**European cardholders September 2013European**	**284,807 transactions**

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

	Cardholder	
[7]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[8]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[9]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[10]	**Not mentioned**	**60.000 transactions in across 12 attributes.**
[11]	**This study used two datasets to run through the experiments. The raw dataset and the new dataset were created by data transformation and data reduction.**	**Not mentioned**
[12]	**E-COMMERCE company in china, it consists of fraudulent and legitimate B2C transactions from November 2016 to January 2017.**	**The original data set contains more than 30,000,000 individual transaction with 62 attributes for each record**
[13]	**Dataset emerges from Kaggle Machine Learning.**	**dataset presents 3075 transactions with 12 features of transactions in CSV file**
[14]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[15]	**Not mentioned**	**containing 284,807 transactions.**
[16]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[17]	**a real dataset obtained from Europay International.**	**The dataset has 1, 00,000 records and 9 attributes.**
[18]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[19]	**German credit card fraud dataset**	**almost 1000 transaction- 20 attributes**
[20]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[21]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[22]	**European cardholders September 2013European Cardholder**	**284,807 transactions**
[23]	**European cardholders September 2013European Cardholder**	**284,807 transactions**

Table 2: the data set source and size

4. Conclusion

Because of the seamless, simple, and convenient usage of e-commerce, digitalization is growing popularity these days.

It became a very common and simple form of payment. People prefer e-payments and e-shopping. Since it is more convenient in terms of time, transportation, and so on As a result of the massive use of e-commerce, there has also been a significant increase in credit card fraud. Fraudsters try to Misuse of a credit card and the lack of transparency in online payments are two issues that need to be addressed. As a result, combating fraudsters' activities has become extremely difficult. The major goal is to keep credit cards transactions safe so that consumers can safely and easily utilise e-banking.

In today's world, one of the most important aspects of banking is fraud detection. Fraud is one of the most significant concerns in terms of monetary losses, not only for merchants but also for individual. Applying data quality dimensions and experimenting with different strategies to partition datasets with machine learning algorithms will result in the best performance and accuracy in detecting credit card fraud. to accurately identify frauds, quickly discover fraud cases streaming, and the ability to detect online fraud in real-time, requiring less time for variation approaches, and detecting hidden correlations in data. The results of Traditional methods have no high accuracy, its results not guaranteed, and it takes more time to process.

Now the challenges we forced with machine learning have two faces: first is to use the algorithm that detect credit card fraud automatically, the ability to accurately identify frauds, the ability to quickly detect fraud cases streaming and the ability to detect online fraud in real-time, the reduction of time required for varication methods, and the identification of hidden correlation in data. And second, the fraudsters are constantly improving their methods, this is a difficult and serious situation, where the failure to develop the methods used to detect credit card fraud will lead to great losses, either for the financial institution or for individuals.

Most of previous systematic papers ignored the use of deep learning, our research recommended in the future work to use deep learning methods, Where Credit card fraud has been detected using machine learning techniques, although no fraud detection system has been able to achieve high efficiency to yet. Deep learning has recently been used to solve complex issues in a variety of fields. The performance of deep learning methods for credit card fraud detection is compared to machine learning algorithms, results reveal that the deep learning methods outperform traditional machine learning models, implying that the deep learning approaches can be used to detect credit card fraud in real-world situations. And also, this paper recommended to cover the data quality dimension in dataset because of their impact on obtaining better results [24].

REFERENCES:

1. Uchhana, N. Ranjan, R. Sharma, S. Agrawal, D. Punde, A., *Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection.* International Journal of Innovative Technology and Exploring Engineering 2021. **10**(6): p. 101-108.

2. Chakshu. V, Chand. S., *Credit Card Fraud Detection And Analysis Using Machine Learning Algorithms.* International Journal Of Innovations In Engineering Research And Technology 2021. **8**(5): p. 121-127.

3. Sadineni, P.K. *Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms*. in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. 2020. IEEE.

4. Ignatious. J, Kulkarni. Y, Bari. S, Naglot. D., *Comparative Analysis of Machine Learning Algorithms for Credit Card Fraud Detection.* international jornal of computer sciences and engineering, June 2020. **8**(6): p. 6-9.

5. Anand, H., R. Gautam, and R. Chaudhry, *Credit Card Fraud Detection Using Machine Learning*. 2021, EasyChair.

6. Rout, M., *Analysis and comparison of credit card fraud detection using machine learning*, in *Advances in electronics, communication and computing*. 2021, Springer. p. 33-40.

7. Nadim, A.H., et al. *Analysis of Machine Learning Techniques for Credit Card Fraud Detection*. in *2019 International Conference on Machine Learning and Data Engineering (iCMLDE)*. 2019. IEEE.

8. V Kumar K S, V.K.V.G., V Shankar A, Pratibha K, *Credit card fraud detection using*

https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/2
DOI: https://doi.org/10.54623/fue.fcij.7.1.2

machine learning Algorithms. International Journal of Engineering Research & Technology, 2020. **9**(07): p. 1526-1530.

9. Manohar s, Bedi. A., Kumar. S, Singh. Kr. S., *Fraud detection in credit card using machine learning techniques.* Innternational Research Journal of Engineering and Technology. , April 2020. **07**(04): p. 1786-1791.

10. Sadgali, I., S. Nawal, and F. BENABBOU. *Fraud detection in credit card transaction using machine learning techniques*. in *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*. 2019. IEEE.

11. Yee, O.S., S. Sagadevan, and N.H.A.H. Malim, *Credit card fraud detection using machine learning as data mining technique.* Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 2018. **10**(1-4): p. 23-27.

12. Xuan, S., et al. *Random forest for credit card fraud detection*. in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*. 2018. IEEE.

13. Adepoju, O., J. Wosowei, and H. Jaiman. *Comparative evaluation of credit card fraud detection using machine learning techniques*. in *2019 Global Conference for Advancement in Technology (GCAT)*. 2019. IEEE.

14. Dornadula, V.N. and S. Geetha, *Credit card fraud detection using machine learning algorithms.* Procedia computer science, 2019. **165**: p. 631-641.

15. Choudhury, T., et al. *An Efficient Way to Detect Credit Card Fraud Using Machine Learning Methodologies*. in *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2018. IEEE.

16. Campus, K., *Credit card fraud detection using machine learning models and collating machine learning models.* International Journal of Pure and Applied Mathematics, 2018. **118**(20): p. 825-838.

17. Suryanarayana, S.V., G. Balaji, and G.V. Rao, *Machine learning approaches for credit card fraud detection.* Int. J. Eng. Technol, 2018. **7**(2): p. 917-920.

18. Puh, M. and L. Brkić. *Detecting credit card fraud using selected machine learning algorithms*. in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2019. IEEE.

19. Patil, S., V. Nemade, and P.K. Soni, *Predictive modelling for credit card fraud detection using data analytics.* Procedia computer science, 2018. **132**: p. 385-395.

20. Husejinovic, A., *Credit card fraud detection using naive Bayesian and c4. 5 decision tree classifiers.* Husejinovic, A.(2020). Credit card fraud detection using naive Bayesian and C, 2020. **4**: p. 1-5.

21. Trivedi, N.K., et al., *An efficient credit card fraud detection model based on machine learning methods.* International Journal of Advanced Science and Technology, 2020. **29**(5): p. 3414-3424.

22. Joshi, A., S. Soni, and V. Jain, *An Experimental Study using Unsupervised Machine Learning Techniques for Credit Card Fraud Detection.*

23. Garg, V., S. Chaudhary, and A. Mishra, *Analysing Auto ML Model for Credit Card Fraud Detection.* International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN, 2021: p. 2347-5552.

24. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). Deep learning methods for credit card fraud detection. *arXiv preprint arXiv:2012.03754*.