Supported by tetfund

A HYBRIDIZATION Of MACHINE LEARNING AND DEEP LEARNING MODEL FOR DETECTING CREDIT CARD FRAUDULENT ACTIVITIES

Agu, Edward .O. ; Andrew Ishaku .W.

Computer Science Department, Federal University Wukari, Taraba, Nigeria
Corresponding author: aguedwardo@gmail.com

Received: February 11, 2023 **Accepted:** April 15, 2023

Abstract:

Fraud has for decades been a major problem for merchants, especially for the online business sector that deals with credit cards.The challenging problem of fraud detection is that fraudsters make all possible efforts to make their transaction more legitimate. Another difficulty is that the number of legitimate records is far greater than the number of fraudulent cases. Such unbalanced sets require additional precautions from the data analyst. An effective technique for accurate fraud detection lies in developing dynamic systems that evolve to new fraud patterns. This implies that fraud detection must evolve continuously, and much faster than fraudsters which necessitate the hybridization method used in this research to tackle credit card fraudulent activities' detection. A credit card fraud dataset used was obtained from the Kaggle machine repository. The result achieved showed that the Random Forest Classifiers as a machine learning proffers a significant performance for data split of 75:25 training to testing distribution with an astonishing result percent of 98% than the Artificial Neural Network as a deep learning which depicts an accuracy score of 0.9184 value, which is equivalent to 92%. This revealed the viability of the hybridized model used in this research for detection of credit card fraudulent activities within the record of a financial transaction with higher percentage accuracy compare to other researches.

Keywords: Fraudulent, detection, credit-card, machine-learning, deep-learning

Introduction

Fraud has for decades been a major problem for merchants, especially for the online business sector. Credit card fraud can be said to be the action of an individual who uses a credit card for personal reasons without the consent of the owner of the credit card and with no intention of repaying for the purchase made or a criminal deception with the intent of acquiring financial gain (Bhatla, 2003). This implies that there is a need for adequate security of data transmittedover the network by mitigating the tools and methods applied (Agu *et. al*, 2017; Francisca *et. al*, 2015). Contrary to what many consumers believe, merchants are responsible for paying the bill when a fraudster steals goods or services in a consumer-not-present transaction, such as an online payment. A chargeback occurs when a consumer claims that he/she did not get the products or services requested, or that the order was placed by a fraudster. If the company cannot rebut this claim, the money will have to be returned to the consumer's account and the product is lost (if it has been shipped). Moreover, merchants can be subject to chargeback fees and fines from card associations if the chargeback rate is above their thresholds (Montague, 2010).

The challenging problem of fraud detection is that fraudsters make all possible efforts to make their transaction more legitimate. Another difficulty is that the number of legitimate records is far greater than the number of fraudulent cases. Such unbalanced sets require additional precautions from the data analyst. An effective technique for accurate fraud detection lies in developing dynamic systems that evolve to new fraud patterns (Quah, 2008). This implies that fraud detection must evolve continuously, and much faster than fraudsters.

In the real-world fraud detection system, the bulk stream of payment requests is quickly scanned by an automated machine learning model, which authorizes a transaction. Supervised methods are by far the most applied methods in fraud detection, where dataset labels are exploited for training a classifier. For this, the study explores the viability of a random forest (as a machine learning model) and the artificial neural network (as the deep learning model) on a credit card dataset obtained from Kaggle to solve the issue of credit card fraud.

Aim and Objectives

The aim of this study is to develop a hybrid machine learning and deep learning model for detecting credit card fraudulent activities. To achieve the targeted goal, the below objectives serve as a supplement to:

1. effectively filter and cleanse the dataset using the appropriate data preprocessing model.
2. apply the random forest algorithm and artificial neural network to credit card fraud analysis.
3. validate and compare the performance of the model using the accuracy models.

Literature Review

Shizhe *et al*., (2020) developed a novel method to implement cross features based on the convolutional neural network for credit card fraud detection. The model extracts important cross features and generates cross-feature embedding from structured data which reduces the need to generate hand-crafted cross features via a pooling layer as the downsampling technique to map the features and to further preserve important cross features before the pooled feature are then flattened into a single vector. The single vector was then fed into a Feed-Forward Artificial Neural Network that generates the final cross-feature embedding with the Rectified Linear Unit (ReLU) utilized as the non-linear activation function. The experimental results show that their method improved the performance of predicting loan default probability compared with the methods based on classical machine learning algorithms that were widely used in loan default prediction with an accuracy score of 0.765 for the German dataset and 0.783 for the Taiwan dataset (Shizhe *et al*., 2020). The authors further revealed that to some extent, their model retains interpretability for raw feature vectors due to the logistic classifier.

Deepika and Senthil, (2021) worked on credit card fraud detection using a Moth-flame earthworm optimization algorithm-based deep belief neural network. The author's implementation uses a database with the credit card transaction information that upon queries, the records are passed through data pre-processing. Hence, a log transformation was applied over the database for data regulation in the pre-processing step and the appropriate features were selected by the information gain criterion. After the feature selection stage, the selected features were utilized to train the classifier using the adopted moth-flame earthworm optimization-based deep belief network (MF-EWA-based DBN). The weights for the classifier were selected by the newly developed moth-flame earthworm optimization algorithm (MF-EWA). At the end of their analysis, the authors reported that their model “MF-EWA-based DBN” classifier improved detection with an astounding performance of 85.89%.

Yiheng & Weidong (2021) proposed some entropy methods in constructing a hybrid model for improving loan default prediction. The authors conducted some pre-processing based on Random Forest and thus combined the Logistic Regression algorithm and Artificial Neural Network model to improve the predictive performance of Random Forest based on some actual data collected from a rural commercial bank under the condition that loan quality directly affects the profitability of the bank. The authors' experimental results revealed that their proposed combined model outperforms the benchmarked classifier and stacking method on four evaluation metrics: accuracy (ACC), the Area Under the Curve (AUC), Kolmogorov-Smirnov statistic (KS), and Brier score (BS) from 88.11% to 91.08%. They concluded that their model is superior to a state-of-the-art ensemble model, stacking.

Mehul *et al*., (2021) worked on a loan default prediction using Decision Trees and Random Forest. The author used a publicly available Lending Club dataset from the Kaggle machine learning repository and preprocessed it. According to the authors, the dataset covers approximately 22 Lakh loans funded by the platform between 2007 and 2015. To gauge the effectiveness of their model, the authors split the data into 70% training and 30% test sets. The result of the author's analysis revealed a 73% accuracy for the Decision Tree and 80% accuracy for the Random Forest Classifier.

Summary of Related Works for Loan Default

Authors	Algorithms	Best Model	Accuracy
Shizhe *et al*., (2020)	Convolutional neural network.	Convolutional neural network.	78% and 76%
Deepika and Senthil, (2021)	moth-flame earthworm optimization-based deep belief network (MF-EWA-based DBN)	moth-flame earthworm optimization-based deep belief network (MF-EWA-based DBN)	85.89 %
Yiheng & Weidong (2021)	Random Forest, Logistics, Regression and Artificial Neural Network	Artificial Neural Network	91.08%
Mehul *et al*., (2021)	Decision Trees and Random Forest	Decision Trees	80%

Research Gap

The study conducted has revealed that several machine learning and deep learning models have been applied by various researchers for the critical analysis of credit loans before their issuance. Although, these researchers have tremendously shown the viability of their respective models years ago. But as technology advances, likewise, the techniques applied by fraudsters evolve. Thus, to provide an effective and efficient feasible solution to the problem of credit-loan default risks, this study proposed the performance evaluation of machine learning and deep learning classification algorithm namely, the Artificial Neural Network (as the deep learning model) and the Random Forest(as the machine learning model).

Research Methodology

To take advantage of the sheer size of modern datasets, optimizing the scalability and effectiveness of machine and deep learning algorithms concerning the volume of information and problem domain (credit card fraud) while maintaining sufficient statistical efficiency is necessary to provide a feasible solution to the ever-growing fraudulent activities.

Hence, this study developed four methodological approaches that entail data preprocessing and feature selection using correlation metricsin the first phase. The second phase captures the application of the pre-processed data to the model in particular the artificial neural network and the random forest algorithm. The last phase encapsulates the performance evaluation of the model produced by both the artificial neural network and the random forest algorithm.

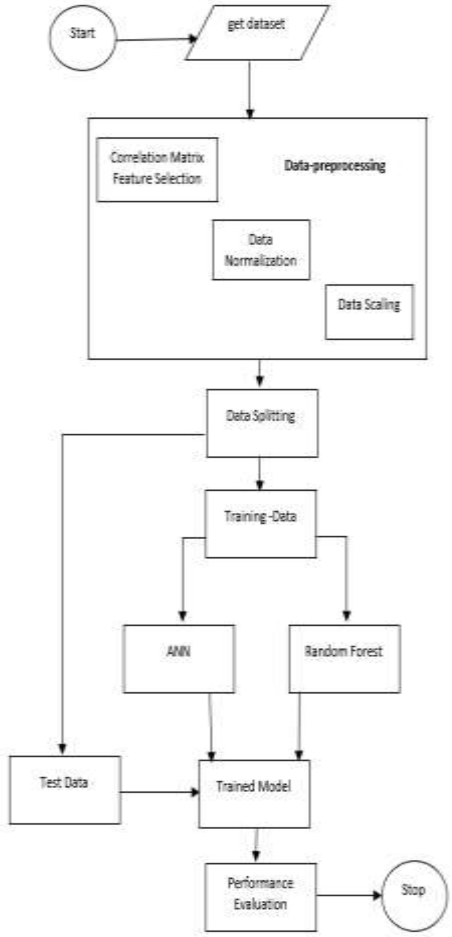


Figure 3.1: research methodology

Data Preprocessing and Feature Selection

For enhancing the performance and precision accuracy of the adopted artificial neural network and the random forest algorithm, it is essential to perform data preprocessing to eradicate irregularity from the sourced dataset. Hence, the data pre-processing steps adopted by this study encapsulate the identification and eradication of Null and Na values, categorical data transformation, scaling (between 0 and 1)and encoding using sklearn min-max scaler, the identification of relevant features based on

Classification Methods

Taking into cognizance the dataset obtained from Kaggle for this experiment, the problem of credit card fraud was identified to be a classification problem as the dataset contains a binary class of a record been of fraud or not. Hence, it becomes essential to identify algorithms that best fit binary classification problems. The algorithm adapted is the artificial neural network and the random forest algorithm.

Artificial Neural Network

An artificial neural network (ANN) is a computational model that emulates the biological neural system to conduct comprehensive data analysis. This study utilized a Multi-layer Perceptron Neural Networks model, which maps a set of input data onto a set of appropriate output data through three layers of neurons through the three layers; namely the input layer, hidden layer, and output layer. Mathematically, the input layer consists of neurons corresponding to predictive variables $\left(x^1x^2, \ldots \ldots x^k\right)$which are connected to neurons in the hidden layer. Each neuron in the hidden layer then sums the data received from the input layer through weighted connections and then modifies the sum by a non-linear transfer function before passing the sum to the output layer. To appropriately train the ANN model, the backpropagation algorithm was utilized, accompanied by the application of the rectified linear function (Relu) as the activation function to the input layer with 256 neurons, then two dense layers as the hidden layerswith 128 and 64 neurons respectively and lastly, the final layer which corresponds to the output layer was given a single perceptron since the classification problem on credit card fraud is a binary type. The output layer utilized the sigmoid function as the activation function with the learning rate and the momentum set to 0.0001 and 0.7 respectively.

Algorithm 1: Artificial Neural Network

Step 1: Passed the input with some weight to the hidden layers $(x^1x^2, \ldots \ldots x^6)$
Step 2: Connect all the inputs to each neuron
Step 3: perform computation at the hidden layers
Step 3.1: Get the summation of all input with their weight (check figure 3.2)
Step 3.2: Get bias (check figure 3.2).
Step 3.3: Get the threshold unit (check figure 3.2).
Step 4: Repeat step 3 for each of the hidden layers
Step 5: Pass the result to an output layer
Step 6: Get predictions from the output layers and hence calculate the performance metrics.
Step 7: Calculate error, i.e., the difference between the actual and predicted output.

Random Forest

Random forest is a Supervised Machine Learning Algorithm that is used widely in Classification and Regression problems. The Random Forest algorithm builds decision trees on different samples and takes their majority vote for classification and average in case of regression. An important feature of the Random Forest Algorithm is that it performs effectively when handling datasets containing categorical variables as in the case of the proposed crime classification problem. The adopted model Random Forest is an ensemble method that combines multiple models to make predictions rather than an individual model using bagging (creates a different training subset from sample training data with replacement with the outcome depending on majority voting) or boosting (combines a weak learner into a strong one by generating a sequential model in a way that the final model has the highest accuracy) techniques.

Algorithm 2: Random Forest Algorithm

```
Input: Training set$\mathbf{D_n}$, number of trees $M > 0$, $\mathbf{a_n} \in \{1,\ldots,n\}$, $\mathbf{M_{try}} \in \{1,\ldots,p\}$, $\mathbf{Node_{size}} \in \{1,\ldots, \mathbf{a_n}\}$, and $x \in X$.
Output: Prediction of the random forest on credit card fraud dataset.
For $j = 1,\ldots,M$ do
    Select $\mathbf{a_n}$ points, with (or without) replacement, uniformly in $\mathbf{D_n}$.
    Set P = (X) the list containing the cell associated with the root of the tree.
    Set $\mathbf{P_{final}} = \emptyset$ an empty list.
    while P = $\emptyset$do
        Let A be the first element of P.
        if A contains less than $\mathbf{Node_{size}}$ points or if all $X_i \in A$ are equal then
            Remove the cell A from the list P.
            $\mathbf{P_{final}} \leftarrow \mathrm{Concatenate}(\mathbf{P_{final}}, A)$.
        else
            Select uniformly, without replacement, a subset $\mathbf{M_{try}} \subset \{1,\ldots,p\}$of cardinality $\boldsymbol{M_{try}}$.
            Select the best split in A by optimizing the CART-split criterion along with the coordinates in $\boldsymbol{M_{try}}$.
            Cut cell A according to the best split. Call AL and AR the two resulting cells.
            Remove cell A from the list P.
            $P \leftarrow Concatenate(P, AL, AR)$.
        end
    end
    Compute the predicted value $\boldsymbol{M_n}(X;\, \Theta_j, \boldsymbol{D_n})$at x equal to the average of the Yi falling in the cell of x in partition $\boldsymbol{P_{final}}$.
end
Compute the random forest estimate m$\boldsymbol{M_n}(X;\, \Theta_1 \ldots \Theta_m, \boldsymbol{D_n})$at the query point x according to Step-1.
```

Performance metrics

To evaluate the performance of the Artificial Neural Network and the Random Forest on the adaptedcredit card fraud dataset. Evaluation parameters such as precision, recall, and accuracy are calculated.

Precision measures the classifier's accuracy. It is the percentage of the number of correctly predicted positive frauds divided by the total number of predicted positive frauds:

$$\boldsymbol{precision} = \frac{TP}{TP + FP}$$

Recall measures the classifier's completeness. It is the percentage of correctly predicted frauds to the actual number of positive frauds on the dataset. Therefore, recall indicates the number of related labels identified:

$$\boldsymbol{Recall} = \frac{TP}{TP + FN}$$

Accuracy is one of the most important metrics of performance evaluation and is measured as a percentage of the number of correctly predicted frauds to the total number of frauds present in the dataset. Thus, the accuracy calculates the ratio of inputs in the test set correctly labeled by theclassifier:

$$\boldsymbol{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Loss Evaluation

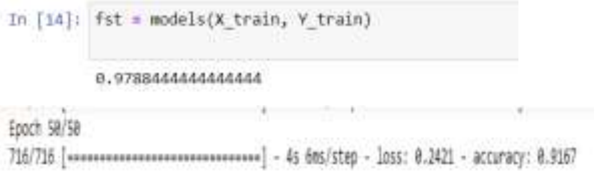
To evaluate the log loss on the prediction of the artificial neural network, the study incorporates the Binary-Cross-Entropy. Binary-Cross-Entropy was chosen due to its suitability in determining loss in classification models where the outcome is either 0 or 1 which corresponds to the class of benign and malignant class of diabetes. The mathematical representation is given as

$$log\ loss = \frac{1}{N}\sum_{i=1}^{N} -(y_i * log(p_i) + (1 - y_i) * log(1 - p_i))$$

Here, p_i is the probability of class 1 that correspond to the fraud, and $(1 - p_i)$ is the probability of class 0 that corresponds to the not fraud class.

Result and Discussion

To enhance the performance of the Artificial Neural Network and Random Forest algorithm, this research carried out data preprocessing to filter data irregularities and thus scaled using the standard scaler from the Sklearn machine learning. After passing the scaled independent and dependent values to the model, the Artificial Neural Network predicted and compiled an overall prediction accuracy of 0.9184 value, which is equivalent to 92% with a step of 716 in 4s 6ms conducted per steps and also a loss metrics based on binary cross entropy of 0.2%. The Random Forest model on the same scaled data produces an accuracy score that surpasses the Artificial Neural Network with an outperforming accuracy score of 0.9788444 value, which is equivalent to 98% when multiplied by 100.



```
In [14]: fst = models(X_train, Y_train)

         0.9788444444444444
```

```
Epoch 50/50
716/716 [==============================] - 4s 6ms/step - loss: 0.2421 - accuracy: 0.9167
```

Figure 4.1: prediction accuracy of Artificial Neural Network and Random Forest Model.

The Artificial Neural Network depicts a graph that shows the accuracy and loss growth as the loss diminishes over 50 training epochs conducted, with an increase in the model prediction upon the same 50 epochs.

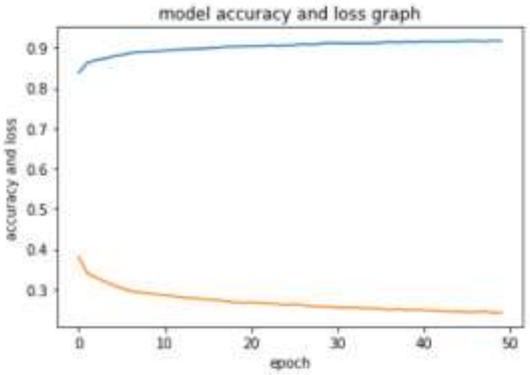
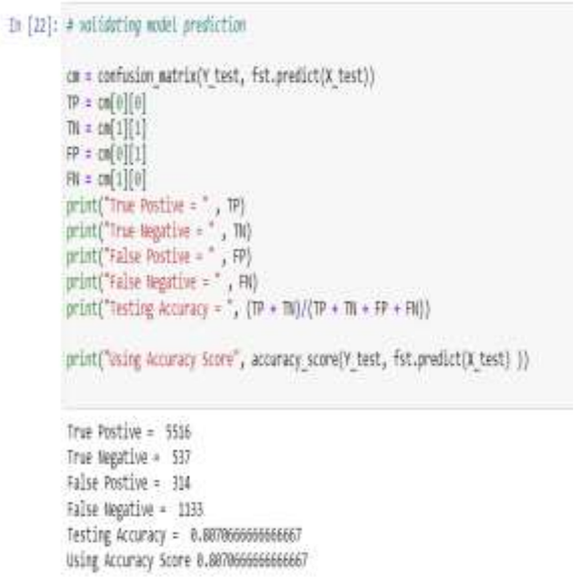


Figure 4.2: Artificial Neural Network learning growth.

To further evaluate the result produced by the best performing algorithm which is the Random Forest Algorithm, the confusion matrix, precision, and recall evaluation metrics were exploited

Confusion Matrix

Accuracy confirmation is one of the most significant aspects of machine learning modules. It depicts the reliability of the model precision. The accuracy of the model based on the confusion matrix of the Sklearn library of machine learning modules was 0.81 as depicted in figure 4.3 below. In percentage, its equivalent is 81%. The accuracy score was compared based on two standards, the confusion matrix, and the accuracy score. Both gave the same accuracy score as shown in the figure below figure 4.3.



```
In [22]: # validating model prediction

         cm = confusion_matrix(Y_test, fst.predict(X_test))
         TP = cm[0][0]
         TN = cm[1][1]
         FP = cm[0][1]
         FN = cm[1][0]
         print("True Postive = " , TP)
         print("True Negative = " , TN)
         print("False Postive = " , FP)
         print("False Negative = " , FN)
         print("Testing Accuracy = ", (TP + TN)/(TP + TN + FP + FN))

         print("Using Accuracy Score", accuracy_score(Y_test, fst.predict(X_test) ))

         True Postive =  5516
         True Negative =  537
         False Postive =  314
         False Negative =  1133
         Testing Accuracy =  0.8070666666666667
         Using Accuracy Score 0.8070666666666667
```

Figure 4.3: confusion matrix

A mathematical validation of the model's accuracy can be calculated using the formulae:

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

from the diagram above

TP = 5516, TF =537, FP = 314, FN = 1133

Hence,

$$\mathbf{Accuracy} = \frac{5516 + 537}{5516 + 537 + 314 + 1133}$$

$$\text{Accuracy} = \frac{6053}{7500}$$

$$\mathbf{Accuracy} = \ 0.8070666667 * 100 = \ 80\%$$

Taking into consideration, the precision of the model, using the formulae,

$$\mathbf{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} = \frac{5516}{5516 + 318} = \frac{5516}{5834}$$

$$\text{precision} = \ 0.945 * 100$$

$$\mathbf{precision} = \ \ 95\%$$

To validate the model recall, the mathematical formulae given below were optimized,

$$\mathbf{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} = \frac{5516}{5516 + 1133} = \frac{5516}{6649}$$

$$\mathbf{Recall} = \ 0.829 * 100 = \ 83\%$$

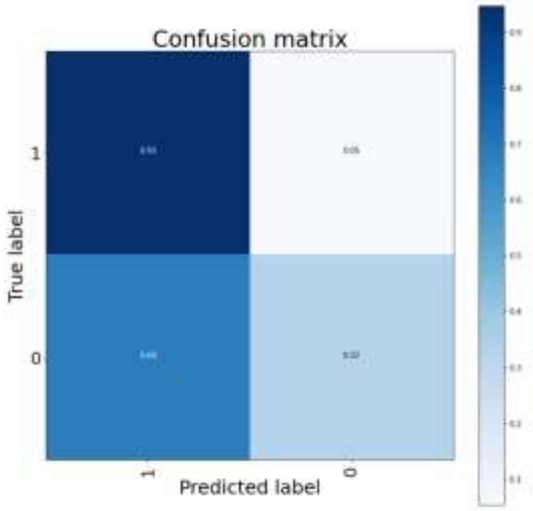


Figure 4.4: Confusion matrix plot

The confusion matrix diagram in figure 4.4 above provides an analysis of the percentage of the result of the position of the True Positive, True Negative, False Positive, and False Negative measures. The top left box represents the correctly predicted record of fraud which were fraud which is 0.95==95%, next to it, is the number of records the model predicted to have fraud but were not fraud, while the bottom left box is the number of records correctly predicted to not having fraud and were not, while the fourth box is the number of records incorrectly predicted to not having fraud.

Conclusion

This paper investigates the performance of the ensemble Random Forest Classifiers and Artificial Neural Network Algorithm in a binary classification of an imbalanced credit card fraud dataset obtained from the Kaggle machine repository. The highly imbalanced dataset is sampled in a hybrid approach where the positive class is oversampled and the negative class under-sampled, achieving two sets of data distributions. The performances of the Artificial Neural Network Algorithm and Random Forest Classifiers were examined on the two sets of data distributions using accuracy, confusion metric, recall, and precision from the confusion matrix module for the best performing model. The result from the experiment conducted revealed that the Random Forest Classifiers show a significant performance for data split of 75:25 training to testing distribution with an astonishing result of percent of 98% than the Artificial Neural Network which depicts an accuracy score of 0.9184 value, which is equivalent to 92%. Hence, this study revealed the viability of the Random Forest Classifier in the detection of fraudulent activities within the record of a financial transaction.

Reference

Agu, E. O., Ejiofor V. E.,Moses T., (2017) A Hybrid Model For Remote Dynamic Data Auditing (RDDA) On Cloud Computing. Journal of Computer Science and Application (JCSA). Vol. 24, No. 1, pp 96-116.

Bhatla, T. P., Prabhu, V., and Dua, A. (2003). Understanding Credit Card Frauds, Cards business review 1 (6) (2003).

Deepika, S., and Senthil, S. (2021). Credit card fraud detection using moth-flame earthworm optimization algorithm-based deep belief neural network International Journal of Electronic Security and Digital Forensics, 14(1), 53-75

Francisca N.O. and Edward O. A,(2015) A Mitigation Technique for Internet Security Threat of Toolkits Attack, International Journal ofComputerScience and Security (IJCSS).ww.cscjournals.org/manuscript/Journals/IJCSS/Volume9/Issue5/IJCSS-1134.pdf. Vol.9, pp225-237

Mehul, M., Aniket, K., Chirag, K., Rachna, J., & Preeti, N. (2021). Loan default prediction using decision trees and random forest. Materials Science and Engineering, 10(22). doi:10.1088/1757-899X/1022/1/012042

Montague, D. (2010). Essentials of Online payment Security and Fraud Prevention, Essentials Series, Wiley, 2010. URL https://books.google.pt/books?id=3IJCmhWztBIC

Quah, J. T., and Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence, Expert Systems with Applications 35 (4) 1721±1732. doi:10.1016/j.eswa.2007.08.093.http://linkinghub.elsevier.com/retrieve/pii/S0957417407003995

Shizhe, D., Rui, L., Yaohui, J., & Hao, H. (2020). CNN-based feature cross and classifier for loan default prediction. International Conference on Image, Video Processing and Artificial Intelligence, 11584. https://doi.org/10.1117/12.2579457

Yiheng, L., & Weidong, C. (2021). Entropy method of constructing a combined model for improving loan default prediction: A case study in China. Journal of the Operational Research Society, 72(5), 1099-1109, DOI: 10.1080/01605682.2019.1702905