A Supervised Approach to Credit Card Fraud Detection Using an Artificial Neural Network

Oluwatobi Noah Akande[1], Sanjay Misra[2(✉)], Hakeem Babalola Akande[3], Jonathan Oluranti[4], and Robertas Damasevicius[5]

[1] Computer Science Department, Landmark University, Omu-Aran, Kwara State, Nigeria
akande.noah@lmu.edu.ng
[2] Department of Computer Science and Communication, Ostfold University College, Halden, Norway
[3] Department of Telecommunication, University of Ilorin, Ilorin, Kwara State, Nigeria
akande.hb@unilorin.edu.ng
[4] Center of ICT/ICE, Covenant University, Ota, Nigeria
jonathan.oluranti@covenantuniversity.edu.ng
[5] Kaunas University of Technology, Kaunas, Lithuania

Abstract. The wide acceptability and usage of credit card-based transactions can be attributed to improved technological availability and increased demand due to ease of use. As a result of the increased adoption levels, this domain has become profitable and one of the most popular targets for fraudsters who use it to conduct regular exploitations or assaults. Merchants and financial processing providers that sell credit cards suffer substantial financial damages as a result of credit card theft. Because of the possibility of large casualties, it is one of the most serious risks to these organizations and individuals. Credit card fraudulent transaction can be viewed as a binary classification task in which a supervised machine learning technique could be used to analyze and classify a credit card transaction dataset into genuine or fraudulent cases. Therefore, this study explored the use of Artificial Neural Network (ANN) for credit card fraud detection. ULB Machine Learning Group dataset that has 284, 315 legitimate and 492 fraudulent transaction were used to validate the proposed model. Performance evaluation results revealed that model achieved a 100% and 99.95% classification accuracy during training and testing respectively. This affirmed the fact that ANN model could be efficiently used to predict credit card fraudulent transactions.

Keywords: Sales forecasting · XGBoost algorithm · Machine learning · Walmart dataset

1 Introduction

The advancement in Information and Communication Technology (ICT) has made it possible for buying and selling to happen via the Internet without any need for face-to-face interaction. Financial institutions have increased the flexibility of transacting businesses online with the aid of innovative solutions supported by credit cards and

H. Florez and M. F. Pollo-Cattaneo (Eds.): ICAI 2021, CCIS 1455, pp. 13–25, 2021.
https://doi.org/10.1007/978-3-030-89654-6_2

mobile banking applications. These solutions have made transacting businesses online easier, faster and have also eradicated long queue waiting time in banks. Thanks to the widespread use of credit cards and the exponential growth of e-services, the volume of credit card purchases has increased significantly [1]. However, the continuous reliance and usage of credit cards and mobile banking applications without strict oversight and verification have opened up many customers to diverse kinds of financial frauds and attacks. The increased credit card transactions during the COVID-19 lockdown gave fraudsters the more opportunities to perpetrate their illicit acts. According to a US based Fidelity National Information Services, the dollar volume of attempted illegal transactions in dollars increased by 35% in April 2020 alone. With US as the largest country of credit card fraud cases, credit card fraud cost the world $24.2 billion in 2018, with credit card fraud transactions estimated to hit $40 billion by 2027 [2]. According to the Unisys protection index, credit and debit card frauds are Americans' top concern, far surpassing terrorist concerns [3].

Credit-card fraud occurs when an individual uses a credit card for personal purposes without the owner's permission and with no intention of repaying the payment. Furthermore, the person who uses the card has no ties to the cardholder or issuer, and has no intention of approaching the card's owner or repaying the transactions received [4]. Credit card fraud can occur when an unauthorized cardholder uses a fake identity to gain the confidence of a bank official, or when stolen credit cards are used [5]. It is an unfair or criminal deceit with the goal of gaining personal benefit [5]. Contrary to popular belief, when a fraudster steals with the use of a credit card, the bill is the responsibility of the retailers [6]. Also, when a customer claims that he did not receive the goods, he ordered for, there will be a need for the retailers to pay back if the claim can be proved by the customer. If the corporation is unable to refute this argument, the money will be returned to the customer's account, and the goods will be discarded (if it has been shipped). Furthermore, if the chargeback rate exceeds the card associations' limits, retailers can be liable to chargeback penalties and penalties [7]. Ten different types of credit card frauds were reported in [26]. Application fraud occurs when a fraudster gains control of an application, obtains the customer's information, creates a phony account, and then conducts transactions. Electronic or manual card imprints: In electronic imprint fraud attempt, the fraudster retrieves the needed information from the card's magnetic strip. this information is then utilized to carry out fraud transactions. in card not present fraud attempt, the hacker does not make use of the actual physical card at the time of the transaction while in counterfeit card fraud attempt, the hacker replicates data available on the magnetic strip of the original card to create a fake card that will be used in the transaction. Lost/stolen fraudulent card attack occurs when the actual owner of the card lost the card and is found by the fraudster or when the fraudster deliberately steals the card from the owner. In card id theft instances, the cardholder's id or credentials is stolen and the stolen credentials are used in perpetrating fraud. Mail non-received card fraud attack occurs when the hacker intercepts a mail sent by the bank to inform the cardholder that his/her card is ready for collection. Here, the true recipient may not receive the mail or the content of the mail may be manipulated such that the intended recipient will receive the mail after the card details have been retrieved. Similarly, in account takeover: attempt, the hacker hijacks the account of the cardholder during the illegal transaction

period. So, the owner of the card won't be aware of the fraudulent transactions going on with his/her account. In fake fraud on website attack, a hacker inserts malicious code into the website of the ATM producing company or bank and uses the information retrieved for fraudulent activities. Conflict between merchants' attack occurs when there is a leak of card information between the card manufacturer, the financial institution and a third party. Generally, credit card frauds can be categorized into two: online fraud and offline fraud; the first is committed by using a stolen credit card for transactions while the second is committed by manipulating victim identification such as credit card numbers, credit card holders' names, expiration dates, and passwords [10].

However, authors in [1] classified credit card fraud into application fraud [8] and behaviour fraud [9]. Application fraud occurs when a fraudster requests for a new card using another person's identity. Behavior fraud occurs when a fraudster steals or forges a card or carries out illegitimate transactions with or without the credit card. The most popular form of behaviour fraud occurs when a stolen credit card is used for unauthorized transaction. The method of determining whether a transaction carried out using credit card is legitimate or fake is known as credit card fraud identification [4, 10]. To reduce fraud losses, a sophisticated fraud detection system with a cutting-edge fraud detection model is considered important [1]. Regardless of the fraud identification model adopted, fraudulent transactions which are always the minority-class samples must be distinguished from the legitimates transactions which are always the majority-class samples [11, 12]. However, instances of normal transactions are always more than the suspicious transactions in the fraudulent transactions class; this makes the classification task a delicate but surmountable task [10, 13–15]. Nevertheless, several innovative solutions such as the Address Verification System (AVS), Chip and Pin identification, and Card Verification Code (CVV) have been explored to deter credit card fraud [6]. However, most of these solutions have been compromised by the fast fingers of hackers. Therefore, the advancement of fraud detecting approaches is critical and fraud detection techniques must continue to grow at a quicker rate than fraudsters. Supervised and unsupervised machine learning approach have been adopted in the literature to detect credit card frauds. In the supervised approach, transactional data records are grouped into fraudulent and non-fraudulent transactions while in unsupervised approach, secret trends in non-labeled transactional data are identified with the help of machine learning algorithms. Account numbers, credit card and payment forms, transaction location and time, customer name, merchant code, transaction size, and so on are some of the transaction information that can be found in these transactional data records. This information can be used as pointers to decide whether a transaction is illegitimate or legal, as well as to investigate outliers that might indicate a suspicious event. A supervised approach to detecting credit card fraud using Artificial Neural Networks is presented in this study. The dataset employed to train and test the resulting ANN model contains credit card transactions made by European cardholders in September 2013. This dataset has 284,807 transactions that occurred in two days; 284, 315 of these are legit credit card transactions while the remaining 492 are fraudulent credit card transactions.

2 Related Works

Machine Learning (ML) models are used by card issuers and network providers to detect credit card fraud. Despite the fact that much research has been done in both industry and academia to develop machine learning models, finding effective solutions remains a challenge. Studied on security in banking [16, 17], mobile applications [18, 19] can be found in various papers. ML techniques have been greatly explored to provide solutions to several security threats [20, 21]. A supervised and unsupervised approach for improving credit card fraud detection accuracy was proposed in [22]. Unsupervised outlier scores were computed at various levels of granularity from an annotated credit card fraud detection dataset. The results obtained revealed that combining techniques from both supervised and unsupervised techniques could improve the accuracy of credit card fraud detection. RIBIB, a cost-sensitive Risk Induced Bayesian Inference Bagging model for credit card fraud detection was proposed in [15]. The proposed model is made up of a cost-sensitive weighted voting combiner, a constrained bag formation process, and a Risk Induced Bayesian Inference method as a base learner. Brazilian bank data was used to validate the proposed technique and resulted to a cost reduction of 1.04–1.5 times. Experiments on UCSD-FICO data show that the model is capable of processing unknown data without the need for fine-tuning of domain-specific parameters. Furthermore, authors in [23] suggested a Bayesian Network Classifier (BNC) algorithm for a credit card fraud detection. The model was created automatically using a dataset from an online payment system. When the results achieved was compared to seven different algorithms, the proposed technique achieved a better classification performance. To detect fraudulent credit card transaction behavior, authors in [24] proposed an ensemble model focused on sequential data processing using deep RNN and a voting system based on ANN. The proposed model was more effective in terms of classification time. Moreover, a new hybrid approach built on the divide-and-conquer concept to address the issue of class imbalance was proposed in [25]. The proposed model attempts to exclude minority class outliers as well as a large number of majorities so as to achieve a better classification accuracy. After that, a non-linear classifier was used to deal with this complicated overlapping subset in order to separate them well. The results obtained was better than similar works. Furthermore, authors in [6] investigated the use of both manual and automated classification, as well as providing insights into the whole implementation process and comparing various machine learning processes. As a result, the paper will assist researchers and professionals in the creation and implementation of data mining-based systems for fraud detection and other issues. This project provided the fraud analysts with not only an automated method, but also insights into how to improve their manual revision process, resulting in overall superior results. This study explored the classification prowess of ANN for credit card fraud detection. ULB credit card transactions dataset was used to validate the proposed model. The dataset has 284,807 transactions with 284, 315 being legit credit card transactions while the remaining 492 are fraudulent credit card transactions.

3 Methodology

An ANN based credit card fraud detection model is presented in this study. The model is expected to be able to analyze credit card transactions and determine whether the transaction is legit or that the transaction is a fraudulent one. This section outlines the experiment used for creating the detection model; this involves dataset collection and exploration, feature scaling, model training and testing as well as the performance evaluation.

3.1 Data Collection and Exploration

The dataset employed in this study was retrieved from ULB Machine Learning Group. The dataset contains credit card transactions made by European cardholders in September 2013. It contains record of 284,807 transactions that occurred in two days; 284, 315 of these are legit credit card transactions while the remaining 492 are fraudulent credit card transactions. As a result, the positive class (fraud cases) accounts for 0.172 percent of all transactions. The evidence was somewhat unbalanced and biased toward the optimistic side. It only has numerical (continuous) input variables, which are the result of a feature selection transformation using Principal Component Analysis (PCA) that yielded 28 principal components. In this analysis, a total of 30 input features are used. Owing to confidentiality concerns, the specifications and context information for the features cannot be shared. The seconds elapsed between each transaction and the first transaction in the dataset are stored in the time function. The transaction sum is represented by the 'amount' function. The 'class' takes a value 1 for positive fraudulent cases and 0 for non-fraudulent cases. The data exploration was carried out to understand the various features of the dataset better. These were visualized so as to further examine the related features that will be used for the fraud detection.

3.2 Feature Scaling

One of the most important stages in the pre-processing of data prior to constructing a machine learning model is feature scaling. Scaling will make the difference between a bad and a good machine learning model. Machine learning algorithms that calculate distances between data include feature scaling. When measuring distances, if the function with the higher value range is not scaled, the function with the higher value range takes precedence. Scaling is needed in many algorithms that need faster convergence, such as Neural Networks. The feature scaling technique adopted in this study is the Standard Scaler. This is available in Phython's scikit-learn or sklearn library. Scikit-learn is perhaps Python's most useful machine learning library. Classification, regression, clustering, and dimensionality reduction are only a few of the useful methods in the sklearn library for machine learning and statistical modelling. Each column of the dataset is rescaled to have a 0 mean and 1 Standard Deviation. By subtracting the mean and dividing by the standard deviation, it standardizes a function. If the original distribution is not normally distributed, the relative space between the features will be distorted. The data is scaled when dividing the dataset into the training data and the testing data. By calculating the necessary statistics on the samples in the training set, each function is individually centered and scaled.

3.3 Model Development

Artificial Neural Networks were used to create the proposed credit card fraud detection model (ANN). As seen in Fig. 1, ANNs are multi-layer fully connected neural networks. An input layer, several hidden layers, and an output layer make up all layers. Each node in one layer is connected to the next layer's nodes. The network gets stronger as the number of hidden layers increases.

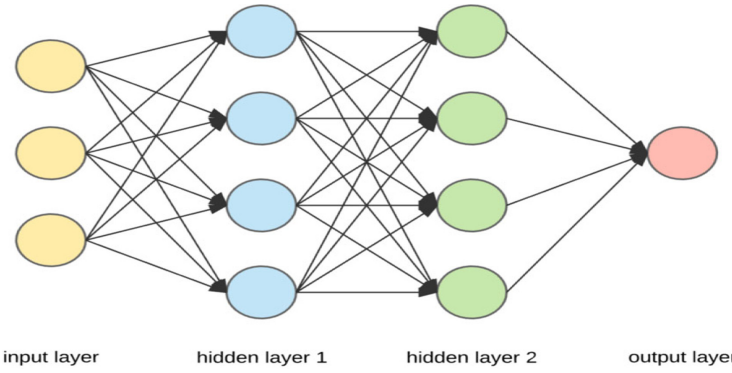

Fig. 1. ANN structure

There is an input layer, a hidden layer (there can be more than 1) and an output layer in the network architecture. Because of the multiple layers, it is also called Multi-Layer Perceptron (MLP). The concealed layer functions as a "distillation layer," extracting valuable patterns from the inputs and passing them on to the next layer to be revealed. It makes the network quicker and more efficient by distinguishing only critical information from the inputs and discarding the redundant data. A given node uses a non-linear activation function to process the weighted number of its inputs. This is the node's output, which is then used as an entry by another node in the next layer. The signal travels from left to right, with the final output calculated by repeating the procedure for all nodes. The model was built using Keras and TensorFlow library. TensorFlow is an open-source machine learning framework that runs from start to finish. It is a simple concept. It is a vast and adaptable ecosystem of software, databases, and other resources that provide high-level APIs for workflows. Keras, on the other hand, is a sophisticated neural network library that uses TensorFlow, CNTK, and Theano as its foundation.

3.4 Training and Testing of the Model

After building the ANN model, the next stage in the report is to train the model. The training process will go through the dataset for a specified number of iterations called epochs, which was defined from the onset with the epochs statement. The batch size was also set using the batch size argument. The number of epochs used in training the model was 300 epochs and the batch size was 2048. The dataset was further divided into 70% for training and 30% for testing. The training dataset was further divided into

80% for training and 20% for dataset validation. The validation dataset was used to provide an unbiased evaluation of a model fit on the training dataset while tuning model hyper parameters. It was used during the training of the dataset. In summary, training this deep neural network involves learning the weights associated with all the edges. So, the training task is aimed at teaching the model how to learn the weights. The training procedure works as follows:

- Initialize the weights for all nodes at random.
- Execute a forward pass using the current weights for each training example, and measure the contribution of each node as it moves from left to right. The value of the last node is the final product.
- Using a loss function, compare the final result to the original goal in the training data and measure the error.
- Make a backwards pass from right to left and use backpropagation to spread the error to each particular node. Calculate each weight's contribution to the error and use gradient descent to adjust the weights. Reverse the error gradients, beginning with the last sheet.

Performance metrics are used to evaluate the performance of any model, to test the performance of the proposed approach the following metrics are used:

- Accuracy: Accuracy refers to the closeness of the measurements to a particular value. It was calculated using Eq. (1):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{1}$$

- Precision: is the number of valid instances among all the positive data used. It was calculated using Eq. (2):

$$\text{Precision} = \text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

- Recall: these also measures the valid instances that were retrieved. It was calculated using Eq. (3):

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

- F1-Score: This is the harmonic mean of the precision and recall. It was calculated using Eq. (4):

$$\text{F1 - Score} = \frac{Precision \cdot Recall}{Precision + Recall} \tag{4}$$

4 Results and Discussion

Majorly, this section narrates the results obtained from the data exploration stage, an overview of the ANN model generated with Phython's Keras and the performance evaluation of the proposed credit card fraud detection model.

4.1 Data Exploration

Understanding the features available in the dataset will determine what can be done with the dataset. Data exploration allows us to visualize the content of the dataset so as to know the relationship between the features. It was while exploring the dataset, that we observed that it has 284315 legit credit card transactions and 492 fraudulent credit card transactions. Furthermore, the presence or absence of missing values were also examined. Interestingly, the dataset has no missing values. After-wards, the distribution of the amount and the time each credit card transactions occur was also visualize. This is shown in Fig. 2. Afterwards, the histogram diagram of the fraudulent transactions and the non-fraudulent transactions were also visualized as shown in Fig. 3. This was done to access how the data were distributed. From the distributions, we can have an idea of how skewed the features are. Further distributions of the other features present in the dataset were also visualized. Furthermore, the correlation of the 28 features was visualized using a Heatmap as shown in Fig. 4. The correlation matrix also reveals that there is no correlation between either of the V1 to V28 PCA elements. Class, on the other hand, has both positive and negative associations with the V elements, but no association with Time or Number. It was thanks to this visualization that we were able to see the need to reduce the data's skewness.

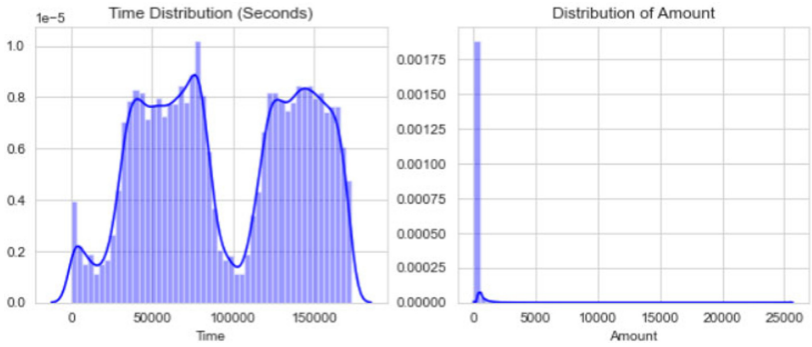

Fig. 2. Time and amount distribution

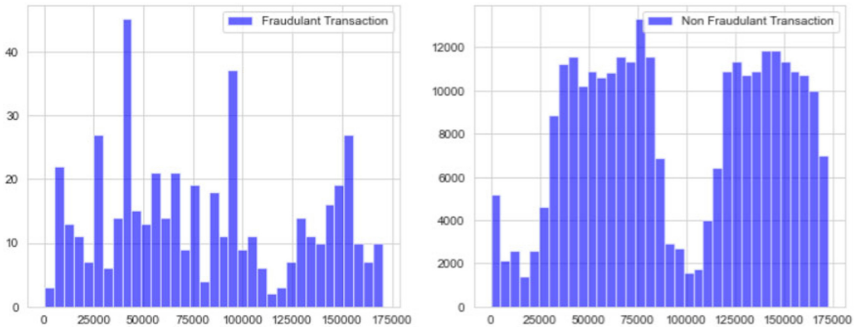

Fig. 3. Histogram of fraudulent and non-fraudulent transactions

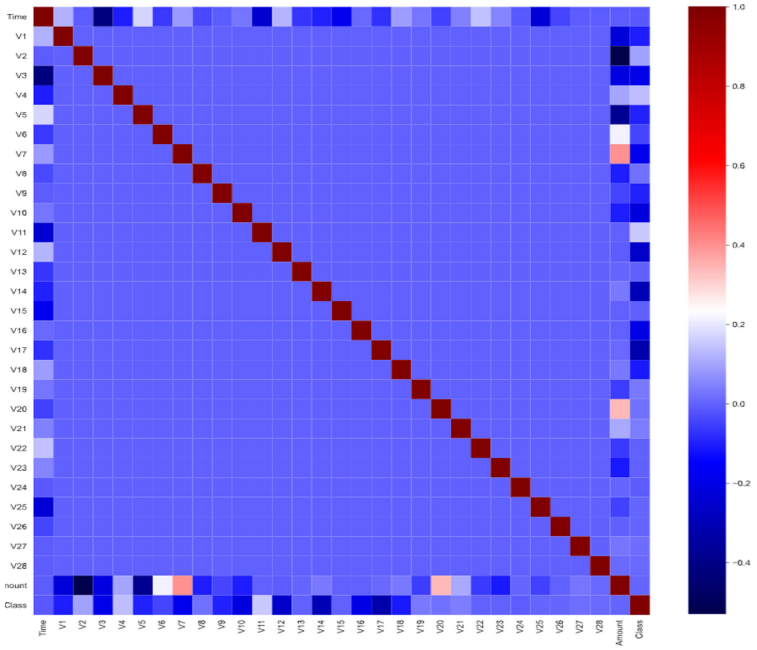

Fig. 4. Heatmap

4.2 ANN Model Built with Phython's Keras

Keras is a deep learning framework that allows quick prototyping and runs on both CPU and GPU. An overview of the ANN model generated with Keras is shown in Fig. 5. From this visualization, it was observed that the resulting model consists of four layers: the first three layers that uses Relu activation function have 256 nodes while the last layer which is the outer layer has one node and uses the sigmoid activation function. The number of trainable and untrainable parameters were also revealed.

```
Model: "sequential_2"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
dense_8 (Dense)              (None, 256)               7936
_________________________________________________________________
batch_normalization_6 (Batch (None, 256)               1024
_________________________________________________________________
dropout_6 (Dropout)          (None, 256)               0
_________________________________________________________________
dense_9 (Dense)              (None, 256)               65792
_________________________________________________________________
batch_normalization_7 (Batch (None, 256)               1024
_________________________________________________________________
dropout_7 (Dropout)          (None, 256)               0
_________________________________________________________________
dense_10 (Dense)             (None, 256)               65792
_________________________________________________________________
batch_normalization_8 (Batch (None, 256)               1024
_________________________________________________________________
dropout_8 (Dropout)          (None, 256)               0
_________________________________________________________________
dense_11 (Dense)             (None, 1)                 257
=================================================================
Total params: 142,849
Trainable params: 141,313
Non-trainable params: 1,536
_________________________________________________________________
```

Fig. 5. An overview of ANN model built with Phython's Keras

4.3 Performance Evaluation of the Proposed Model

After training the model with the training set and the validation set, the next task is to use the test dataset set to get an unbiased evaluation of a final model fit on the training dataset. To get the performance of the model, Accuracy, Precision, Recall, F1score and Support were used as the evaluation metrics. Results obtained as shown in Fig. 6 revealed that the proposed model achieved an accuracy of 100% and 99.95% for the training and testing stage respectively (Fig. 7).

```
Train Result:
================================================
Accuracy Score: 100.00%
________________________________________________
Classification Report:
                    0      1  accuracy  macro avg  weighted avg
precision        1.00   1.00      1.00       1.00          1.00
recall           1.00   1.00      1.00       1.00          1.00
f1-score         1.00   1.00      1.00       1.00          1.00
support    159204.00 287.00      1.00  159491.00     159491.00
________________________________________________
Confusion Matrix:
 [[159204      0]
 [     1    286]]
```

Fig. 6. Performance evaluation result for the training stage

```
Test Result:
================================================
Accuracy Score: 99.95%
________________________________________________
Classification Report:
                    0       1   accuracy   macro avg  weighted avg
precision        1.00    0.89       1.00        0.94          1.00
recall           1.00    0.81       1.00        0.90          1.00
f1-score         1.00    0.85       1.00        0.92          1.00
support      85307.00  136.00       1.00    85443.00      85443.00
________________________________________________
Confusion Matrix:
 [[85293    14]
 [   26   110]]
```

Fig. 7. Performance evaluation result for the testing stage

5 Conclusion

The widespread use of cashless transactions has resulted in an influx of transaction data, necessitating the use of advanced machine learning models to detect fraud. Fraud identification is usually a supervised learning process that classifiers do. Classifier prediction accuracy is determined by the quality of the data used to train them. The massive transaction data generated by consumer purchases is used to train classifiers. This massive volume of data serves as a vast training base for the classifier, allowing it to perform well. The use of supervised techniques is based on a compilation of previous transactions for which the transaction mark is identified. The mark is either genuine or fake in credit card fraud identification issues. The sticker is normally discovered after the fact, either as a result of a consumer complaint or as a result of a credit card issuer audit. Supervised approaches use branded past transactions to learn a fraud prediction model, which returns the possibility of a new transaction becoming a fraud for every new transaction. This study explored the use of ANN for credit card fraud detection. The dataset used contains 284,807 where 284, 315 of these are legit credit card transactions while the remaining 492 are fraudulent credit card transactions. The model achieved a 100% and 99.95% classification accuracy during training and testing respectively. This showed that ANN model could be efficiently used to predict credit card fraudulent transactions.

Acknowledgements. Authors appreciate Covenant University Centre for Research, Innovation and Development for sponsoring the publication of this article.

References

1. Zhang, X., Han, Y., Xu, W., Wang, Q.: HOBA: a novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Inf. Sci. **557**, 302–316 (2021). https://doi.org/10.1016/j.ins.2019.05.023
2. Card Fraud Worldwide 2010–2027. https://nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2019. Accessed 20 Apr 2021
3. Unisys Security Index (2017). http://www.app5.unisys.com/library/cmsmail/USI/UnisysSecurityIndex_Global.pdf

4. Bagga, S., Goyal, A., Gupta, N., Goyal, A.: Credit card fraud detection using pipeling and ensemble learning. Procedia Comput. Sci. **173**(2019), 104–112 (2020). https://doi.org/10.1016/j.procs.2020.06.014
5. Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.S., Zeineddine, H.: An experimental study with imbalanced classification approaches for credit card fraud detection. IEEE Access **7**, 93010–93022 (2019). https://doi.org/10.1109/ACCESS.2019.2927266
6. Carneiro, N., Figueira, G., Costa, M.: A data mining-based system for credit-card fraud detection in e-tail. Decis. Support Syst. **95**, 91–101 (2017). https://doi.org/10.1016/j.dss.2017.01.002
7. Montague, D.: Essentials of Online Payment Security and Fraud Prevention. Wiley, Hoboken (2010). Essentials Series. https://books.google.pt/books?id=3IJCmhWztBIC
8. Phua, C., Gayler, R., Lee, V., Smith-Miles, K.: On the communal analysis suspicion scoring for identity crime in streaming credit applications. Eur. J. Oper. Res. **195**(2), 595–612 (2009)
9. Bolton, R.J., Hand, D.J.: Statistical fraud detection: a review. Stat. Sci. **17**(3), 235–249 (2002)
10. Rtayli, N., Enneya, N.: Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. J. Inf. Secur. Appl. **55**, 102596 (2020). https://doi.org/10.1016/j.jisa.2020.102596
11. Johnson, J.M., Khoshgoftaar, T.M.: Survey on deep learning with class imbalance. J. Big Data **6**(1), 1–54 (2019). https://doi.org/10.1186/s40537-019-0192-5
12. Walke, A.: Comparison of supervised and unsupervised fraud detection. In: Alfaries, A., Mengash, H., Yasar, A., Shakshuki, E. (eds.) Advances in Data Science, Cyber Security and IT Applications: First International Conference on Computing, ICC 2019, Riyadh, Saudi Arabia, December 10–12, 2019, Proceedings, Part I, pp. 8–14. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36365-9_2
13. Krawczyk, B.: Learning from imbalanced data: open challenges and future directions. Prog. Artif. Intell. **5**(4), 221–232 (2016). https://doi.org/10.1007/s13748-016-0094-0
14. de Sá, A.G.C., Pereira, A.C.M., Pappa, G.L.: A customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. (2018). https://doi.org/10.1016/j.engappai.2018.03.011
15. Akila, S., Srinivasulu, R.U.: Cost-sensitive risk induced Bayesian inference bagging (RIBIB) for credit card fraud detection. J. Comput. Sci. **27**, 247–254 (2018). https://doi.org/10.1016/j.jocs.2018.06.009
16. Osho, O., Mohammed, U.L., Nimzing, N.N., Uduimoh, A.A., Misra, S.: Forensic analysis of mobile banking apps. In: Misra, S., et al. (eds.) ICCSA 2019. LNCS, vol. 11623, pp. 613–626. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-24308-1_49
17. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. In: Damaševičius, R., Vasiljevienė, G. (eds.) Information and Software Technologies: 25th International Conference, ICIST 2019, Vilnius, Lithuania, October 10–12, 2019, Proceedings, pp. 243–255. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30275-7_19
18. Jambhekar, N.D., Misra, S., Dhawale, C.A.: Mobile computing security threats and solution. Int. J. Pharm. Technol. **8**(4), 23075–23086 (2016)
19. Jambhekar, N.D., Misra, S., Dhawale, C.A.: Cloud computing security with collaborating encryption Indian. J. Sci. Technol. **9**(21), 95293 (2016)
20. Christiana, A.O., Dokoro, H.A., Oluwatobi, A.A.A.N., Oluwatobi, A.E.: Modified advanced encryption standard algorithm for information security. Symmetry **11**(12), 1–17 (2019). https://doi.org/10.3390/sym11121484
21. Akande, N.O., Abikoye, C.O., Adebiyi, M.O., Kayode, A.A., Adegun, A.A., Ogundokun, R.O.: Electronic medical information encryption using modified Blowfish algorithm. In: Misra, S., et al. (eds.) ICCSA 2019. LNCS, vol. 11623, pp. 166–179. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-24308-1_14

22. Carcillo, F., Borgne, Y.L., Caelen, O., Kessaci, Y., Oblé, F.: Combining unsupervised and supervised learning in credit card fraud detection. Inf. Sci. **557**, 317–331 (2021). https://doi.org/10.1016/j.ins.2019.05.042
23. De Sá, A.G.C., Pereira, A.C.M., Pappa, G.L.: Engineering applications of artificial intelligence a customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. **72**, 21–29 (2018). https://doi.org/10.1016/j.engappai.2018.03.011
24. Forough, J., Momtazi, S.: Ensemble of deep sequential models for credit card fraud detection. Appl. Soft Comput. J. **99**, 106883 (2021). https://doi.org/10.1016/j.asoc.2020.106883
25. Li, Z., Huang, M., Liu, G., Jiang, C.: A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. Exp. Syst. Appl. **175**, 114750 (2021). https://doi.org/10.1016/j.eswa.2021.114750
26. Jain, Y., Tiwari, N., Dubey, S., Jain, S.: A comparative analysis of various credit card fraud detection techniques. Int. J. Recent Technol. Eng. **7**, 402–407 (2019)