Journal of Theoretical and Applied Information Technology
15th May 2023. Vol.101. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEEP LEARNING DETECTING FRAUD IN CREDIT CARD TRANSACTIONS

IMANE KARKABA[1*] , EL MEHDI ADNANI[2], MOHAMMED ERRITALI[3]

[1,2,3]Data4Earth Laboratory, Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal 23000, Morocco

E-mail: [1*]imane.karkaba@usms.ma, [2]mehdi.adnani2@gmail.com, [3]m.erritali@usms.ma

ABSTRACT

Fraudulent acts -in the financial sector- cause dramatic losses to companies and individuals. To tackle this conundrum, artificial intelligence trends forthcame to develop a fraud detection system. This paper comes to process fraudulent credit card transactions issue deploying ANN and CNN, two supervised deep learning algorithms that proved efficiency .Yet, two hurdles appear: Constant emersion of new fraudulent patterns and highly-imbalanced dataset. So, sampling techniques are required to balance data, the thing that affects the system performance. Thus, Autoencoder, as an unsupervised deep learning algorithm, was added to compare it to the aforementioned algorithms. Three models were trained on a dataset of 284,807 credit card transactions labeled as fraudulent and legitimate. Various techniques were conducted in the pre-processing phase as normalization, data balancing, and feature selection. In the during-applying model stage, tuning and analysis were conducted on the model parameters to improve the classification decision. Similarly, in the post-applying model stage, a boosting technique was applied. Not only were the models compared in terms of accuracy, precision, recall, and AUC score but also they were based on confusion matrix. Eventually, one model was chosen out of the experimented models based on the robustness of detecting new fraud patterns; especially, the latter demonstrates optimal rates, achieving an f1-score of 93% after classifying not fraud transactions.

Keywords: *Unsupervised Deep Learning, ANN, CNN, Autoencoder, Imbalanced Dataset*

1. INTRODUCTION

Nowadays, the use of online services is increasing dramatically by abandoning the physical traditional manner. The thing that leads to the growth of digital payment services, for the easiness that it brings. Unfortunately, online financial fraud has emerged as well [1], [2]. The more users utilize online financial services the more fraudulent financial activities appear. Financial institutions in general and companies, in particular, are suffering from these malicious activities without being able to detect and prevent them [3]. Financial fraud has become a crucial problem to deal with. We can differentiate between several types of financial fraud [4] such as credit card fraud [5], [6], money laundering [7], [8], and mortgage fraud [9]. However, in this study, we will be dealing with credit card fraudulent transactions. Identifying these fraudulent transactions, when it comes to the credit card, is pretty complicated and not evident due to the behavior changeability of frauds; in other words, they are not sticking to the same pattern. Moreover, fraudsters are attempting to mimic a legitimate client's behavior which complicates the game of fraud detection. Considering the tremendous impact of fraud on the financial industry, several companies and researchers invest too much money and efforts to bring a promising solution to this issue rather than relying on traditional techniques, which are considered inaccurate and time-consuming. Instead, fraud detection systems take place. In this regard, a bunch of solutions are proposed using data mining [10], [11], machine learning [12], and deep learning [13] techniques to overcome this issue by designing an accurate detection system in order to detect accurately fraudulent transactions. The major challenge in this domain is the lack of relevant information on fraudulent transactions which leads, in its turn, to having a highly skewed dataset [14], [15] as well as the changing behavior of transactions. This study will contribute to carrying out a comparison between some supervised and unsupervised deep learning algorithms which are ANN (Artificial Neural Network), CNN (Convolutional Neural Network), and Autoencoder in terms of metrics such as precision, accuracy, f1-score, and AUC. Furthermore, it elaborates how much it improves the results using multiple pre-

processing techniques to cope with various issues such as Oversampling using SMOTE to obtain a balanced dataset, feature selection, and boosting techniques.

The rest of this article is as follows: Section 2 is allotted for describing a bunch of studies concerned with banking anomalies and frauds in the financial domain. Section 3 focuses on the proposed methods we followed in this study. Section 4 sheds light on the outcomes produced by our models. Finally, section 5 summarizes the paper.

2. RELATED WORKS

Over the past years, the world has seen a huge rise in the use of online services. The reason why people adopt credit cards as the first option for online payments. This adoption is seen according to fraudsters as an easy target to steal money by making malicious activities, basically, fraudulent transactions in a way that they imitate the normal client's behavior. The financial institutions and big companies are suffering from this issue since it causes high loss. This fact let them collaborate with researchers by investing money and effort to design fraud detection systems. In the last decade, many techniques and algorithms of machine learning and deep learning were adopted to overpass this problematic. We will discuss some of those techniques in the following paragraphs.

Fraud detection methods are divided into two categories, supervised and unsupervised methods. When it comes to supervised techniques, the model uses the credit card historic data to discover the hidden pattern and classify the new transactions is either fraudulent or normal, whereas unsupervised methods rely on detecting outliers as fraudulent transactions[16].

The k-nearest neighbors (KNN) is based on supervised learning that requires labeled data. It falls under the instance-based learning category because it uses the entire instance to make the classification rather than developing and adjusting weights as in model-based learning algorithms. The principle behind KNN is to calculate the nearest K neighbors based on the distance metric. They usually use Euclidean distance. For instance for a novel coming transaction- First, we calculate the nearest points to it. Afterward, we classify it based on the nearest classes. KNN showed very promising results when it comes to classifying transactions [17].

A comparison was made between the following machine learning algorithms [18]: Logistic Regression (LR), Random Forest, K-Nearest Neighbors (KNN), XG Boost Classifier, and Support Vector Machine (SVM). Dhankhad et al evaluated the said algorithms based on various metrics such as accuracy, F1-score, recall, precision, false-positive rate (FPR), and true-positive rate (TPR). They tackled the skewed dataset problem using the under-sampling technique. Moreover, they showed that the stacking classifier with logistic regression as a meta-classifier has the best score of 0.952 regarding accuracy. Whereas, Random Forest outperforms other algorithms in terms of precision, recall, and F1-score. Besides, SVM underperforms other methods by having the highest rate regarding FPR.

A study was carried out to make a comparison of the three following algorithms [19]: Naïve Bayes, Logistic Regression, and K-Nearest Neighbors. The models were evaluated using TPR, FPR, TNR, and FNR and compared based on various metrics such as accuracy, sensitivity, specificity, precision, and Matthews's correlation coefficient. The skewed dataset issue was handled thanks to the hybrid-sampling technique. The hybrid-sampling technique relies on combining both the under-sampling and the over-sampling methods. The latter technique was applied on a highly unbalanced dataset by under-sampling the non-fraudulent cases and oversampling the fraudulent cases. Furthermore, it showed an improvement in the models' performance. The logistic regression has good performance over un-sampled data; while, it showed a mediocre performance using sampled data. On the other hand, Both Naïve Bayes and KNN performed well and roughly- similarly over all the aforementioned metrics.

The outliers detection technique is widely used [20]. It is categorized into two classes supervised and unsupervised learning. In supervised learning, algorithms classify outliers based on a study and pattern detection of the labeled dataset. In contrast, unsupervised learning based algorithms are pretty similar to clustering methods in dividing data into clusters containing similar points. According to N. Malini and Dr. M. Pushpa, unsupervised learning is much more robust in detecting credit card fraudulent transactions, because of the lack of relevant information for a fraudulent transaction. Therefore, it is trained only using normal transactions [17].

Artificial neural network (ANN) is a robust computational algorithm. It performs very well, especially with a large dataset. It is inspired from the human brain's learning. ANN is a network of perceptrons connected with each other. Each

perceptron is represented by a node. Every node is connected with other nodes in the adjacent layer with a weighed communication, such as, each weight is a float number which is adjusted in the training model's phase. The data is fed into the model through the input layer, that in its turn passes it into a hidden layer long away until the output layer; that is to say, each node attempts to adjust its weights in an appropriate way. ANN is exploited by many researchers for the purpose of credit card fraud detection [21], [22]. Also, it is compared in another survey with logistic regression and ANN outperforms logistic regression [23], [24].

Apapan Pumsirirat and Liu Yan, in their study, propose a deep learning model using Autoencoder architecture [16]. They experiment with it over three datasets. They show that Autoencoder performs better over a large dataset. They reach an AUC score of 96 for the biggest dataset. The procedure of the proposed system is as follows when a novel transaction comes, they retrieve the overall historical record of the user's profile. Then, they train the model on the retrieved profile. Afterward, they validate the given transaction. They do not use labeled data because AE is an unsupervised learning-based algorithm.

Abhimanyu et al made a comparison between four deep learning topologies [13] : Artificial Neural Network (ANN), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM), and Gated Recurrent Unit (GRU), based only on the accuracy score. They show that GRU overperforms other aforementioned algorithms based on 10 folds cross-validation with a score of 0.916. Besides, they mentioned that the number of layers used in each topology significantly affects the score. Moreover, they conclude that LSTM and GRU are adequate and outperform other algorithms when it comes to the modeling of sequential data.

Joy Long-Zong Chen and Kong-Long Lai proposed a Deep Convolutional Neural Network Model for the sake of real-time credit card detection [25]. They compared the proposed model with other machine learning algorithms such as SVM, Logistic Regression, and Random Forest only in terms of accuracy and speed. Their model showed better results in comparison to the machine learning algorithms mentioned before.

In another study, LSTM is examined and evaluated based on accuracy and loss rate [26]. After the hyper-parameter tuning stage to obtain the best result, LSTM exposes better performance in comparison to Autoencoder, SVM, and logistic regression in terms of accuracy of 99.96% and loss rate of 0.21%. Moreover, Random Forest brings the same accuracy but it was much longer regarding speed. Yet, Accuracy alone cannot differentiate between models' performance, especially with a highly skewed dataset.

Despite the huge number of studies that took place to solve this cumbersome problem, there are always difficulties accompanied by financial transactions. The fraudulent act nature is active and changeable meanwhile the fraudulent operations seem to be legal ones. Furthermore, the dataset that can serve to study this problematic is scarcely available and misleading. All these factors bother researchers to reach advances in this domain. In this project, three models based on supervised and unsupervised deep learning are adopted and compared to handle imbalanced classification for the aim of detecting the patterns of fraudulent transactions.

3. PROPOSED MODEL

Challenges are still hampering most of the fraud detection models to achieve optimal results in terms of 'precision', 'recall', 'f1-score', and other reliable metrics for assessing an implemented model's efficiency. This is due to the imbalanced dataset and the existence of useless attributes in the input. Thus, in our journey of looking for operative methods to tackle this issue, our option falls on three algorithms: 'ANN', 'CNN' and 'Autoencoder' which we believe in their pertinence so that we can build our approach.

The source of motivation behind choosing ANN, CNN, and Autoencoder lies under the excellence they equally show in classifying data, regardless of each one's unique characteristics.

- ANN (Artificial Neural Network) is an algorithm that imitates the human brain. The neurons are intertwined in the human brain like the same nodes intertwined in artificial neural networks [27].
- CNN (Convolutional Neural Network) is one of the best deep learning algorithms, able of understanding sophisticated structures, and has reached amazing success in tasks linked to image segmentation, object detection, and computer vision applications. Also, it possesses the potential to exploit spatial or temporal correlation in data. Moreover, CNN has been used in the context of intrusion detection for both feature extraction and classification [28], [29].

- Autoencoder is a kind of artificial neural network utilized to learn data encoding in an unsupervised way. Its goal is to learn a lower-dimensional representation (encoding) for higher-dimensional data, particularly for decreasing dimensionality, by training the network to pick up the most important elements of the input. It contains three modules namely Encoder, Bottleneck and Decoder [30].

Before we immerse into the process of implementing our models, it is mandatory to run a preprocessing operation for our dataset. The latter (dataset) was almost the only one available for our topic matter. It is -credit card fraud data- from a European credit card company. The data includes transactions made by credit card holders in 2013 September. This is the only available dataset until now for the safety of financial companies in this context. More than that, the dataset fits in our project so far. Accordingly, transactions that had happened in two days is shown in the datasets, it is given that the data contains only 492 frauds out of 284,807 transactions which accounts for only 0,172% of all transactions.

Data preprocessing involves various techniques - to make our data suitable for the model-among which we considered 'data validation', as the first step, to checking data quality and quantity, in terms of identifying and handling the missing values, and splitting the dataset. Second, we applied 'normalization', the technique that allowed us to modify and scale the values of numeric columns included in the dataset. Third, we employed the 'feature selection' technique, by dropping the noisy fragments in data and keeping the relevant ones. This was carried out through three main measures. To start with 'correlation' which let us find the link between each variable and target column. Secondly, the variance based technique also attempted to pick the attributes most affecting the results. Ultimately, we based on SVM (Support Vector Machine), accordingly, for selecting the pertinent attributes.

To address this conundrum, a two stage-method took place. In the first stage, our implementation started by loading the dataset from kaggle that we mentioned above. Then, we trained our algorithms (ANN, CNN, and Autoencoder) separately; the thing that allowed us to discover that the 'accuracy ratio' is optimal (90 percent and greater). Consequently, our three models seemed to be skillful, which is not a fact. We realized that we can't judge the efficiency of an implemented model from the high rate of accuracy because it may be nonsense when it has to do with an imbalanced classification problem, in spite of the fact that 'accuracy' is easy to calculate and intuitive to understand as an evaluating metric. The intuition does not work when the distribution of examples to class is sharply skewed. Sometimes the results are incorrect and misleading [31]. This evidence pushed us to try a feature selection technique to regulate data and normalize it, eliminating unnecessary features. After training our models, we realized that ANN and CNN need balanced data as they are based on predictive data diagnosis. A weak spot of the supervised model is its inability to detect frauds that were not available in the historical dataset from which it learns. The reason why the use of techniques such as 'Oversampling', 'SMOTE', etc. is mandatory before feeding our model. Therefore, the need for an unsupervised model is inevitable. That is why Autoencoder is deployed because it does not require a dataset modification.

In the second stage, which is devoted to trying Autoencoder, is characterized by its capacity of transforming the reconstruction error function as 'reconstructed original' input, in other words, the output is changed into reconstructed input. To figure out the problem of true-negative rate augmentation, the three previously described techniques of selecting the most decision impacting variables were implemented. Nevertheless, we chose the last one that relied on the SVM model. After training, our new model several times in a sequential process, a chain of versions was produced. Here, we realize that this prototype (our novel model) is effective since it managed to reduce the true-negative rate. Again, we opt for boosting the last version for its best performance in two steps: First, by taking the reconstruction errors of each variable in each transaction to set up a novel dataset. Second, by implementing the KNN classifier using the reconstruction error, as it is demonstrated in *Figure 1*. Eventually, the results were surprisingly promising.

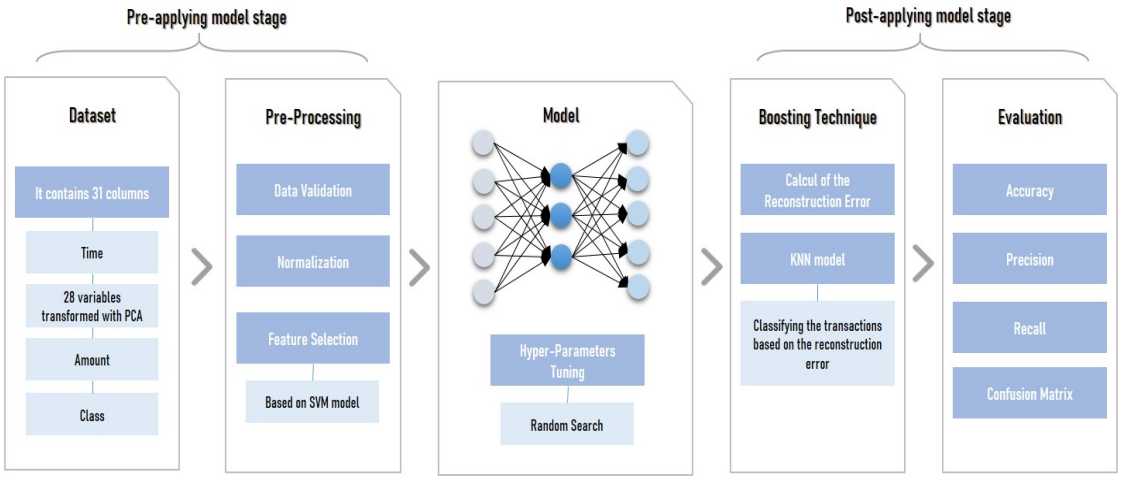


Figure 1: Stages of designing the proposed model based on the Autoencoder architecture

4. RESULTS AND DISCUSSION

4.1 Results

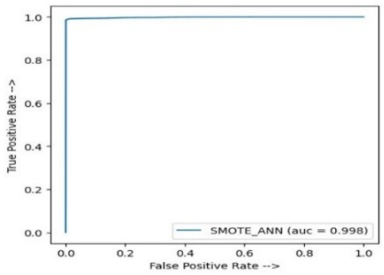
In the current study, three classifiers are developed based on ANN, CNN, and Autoencoder. In order to evaluate the performance of the mentioned classifier models, multiple metrics are used namely accuracy, precision, recall, AUC, and confusion matrix. Besides, 70% of the dataset was dedicated to the training while 30% was left for the test.

For the ANN and CNN cases, before we feed the data into the model, a technique of oversampling is performed on the dataset, called SMOTE, to obtain a sampled dataset distribution of 10:90 (Fraud: Not Fraud). Moreover, a feature selection technique is applied based on the SVM model in order to keep only the columns significantly influencing the decision.

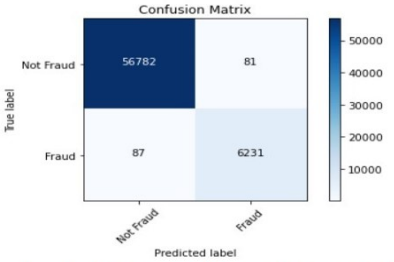
The best performing ANN model trained with 5stratifiedFold cross-validation. This model comprised 7 hidden layers. Every layer is composed of a number of nodes comprised between 8 and 512 nodes. A learning rate of 0.01 was used with an SGD (Stochastic Gradient Descent) optimizer. Furthermore, batch normalization and dropout techniques were utilized between layers for avoiding overfitting. In addition, Relu was adopted as the activation function within the hidden layers whereas Softmax was picked for the output layer. Likewise, the same hyper-parameters were used with the best-performing model based on CNN with a slight difference in the number of nodes in every layer.

For the Autoencoder architecture, the best performing model is received with 3 layers of encoding comprised respectively 64, 16, 16 nodes, and 3 layers of decoding. While the bottleneck involves 8 nodes. The activation function Tanh was used across all the hidden layers whereas Sigmoid was adopted at the output layer. In order to conduct the hyper-parameters tuning, an analysis is carried out on the hyper-parameters. We concluded that the number of the hidden layers, the number of nodes in every layer, the activation function, and the learning rate showed a difference at the level of the output. The false-positive rate and the false-negative rate decrease while the accuracy, precision, and recall increase.

First, the ANN and CNN models were compared after training them on data balanced using SMOTE technique to generate new similar records based on the KNN algorithm. ANN showed the best results in terms of AUC score, precision, recall, and f1-score for classifying fraud and not fraud transactions as it is shown in *Figure 2*(a,c) and *Figure 3*(a,c). Furthermore, the confusion matrices clearly show that the true negatives and positives are high compared to those obtained with the CNN which means the ANN classifies more accurately the transactions (*Figure 2*(b) and *Figure 3*(b)). Then, the ANN model was evaluated in comparison to the Autoencoder model based on the result shown in *Figure 2*(c) and *Figure 3*(c). Autoencoder reach a precision of 1.00 in classifying fraud transactions, which is better than the precision obtained with CNN. Nevertheless, ANN provided a higher recall score of 1.00. However, the Autoencoder has 0 in terms of false positives, which refers to the fact that it did not misclassify a non-fraudulent transaction.



a. AUC score of the model using ANN

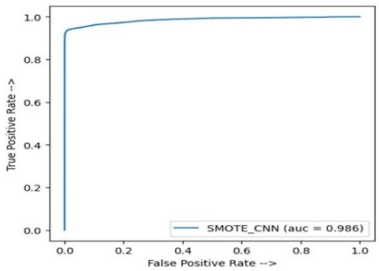


b. Confusion matrix of the model based on ANN

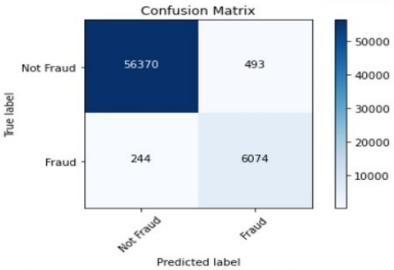
	precision	recall	f1-score	support
0	1.00	1.00	1.00	56863
1	0.99	0.99	0.99	6318
accuracy			1.00	63181
macro avg	0.99	0.99	0.99	63181
weighted avg	1.00	1.00	1.00	63181

c. Classification report of the predictions made by the ANN model

Figure 2: Results of ANN



a. AUC score of the model using CNN



b. Confusion matrix of the model based on CNN

	precision	recall	f1-score	support
0	1.00	0.99	0.99	56863
1	0.92	0.96	0.94	6318
accuracy			0.99	63181
macro avg	0.96	0.98	0.97	63181
weighted avg	0.99	0.99	0.99	63181

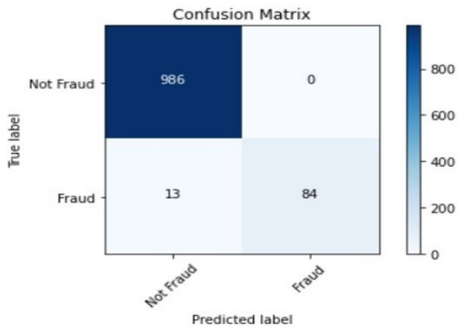
c. Classification report of the predictions made by the CNN model

Figure 3: Results of CNN

4.2 Discussion

In order to prove the efficient model out of the experimented models in the field of credit card fraud detection. The models were evaluated based on multiple metrics such as accuracy, precision, recall, AUC, and the confusion matrix. It is evident from the results demonstrated in *Figure 2*(c) and *Figure 3*(c) that ANN outperforms the CNN model and shows better scores across all the evaluation metrics obtained with the same dataset. For the aim of balancing the dataset, the SMOTE technique was applied by generating new similar records. The

Oversampling technique adopted to balance the data was crucial in making ANN and CNN models train more efficiently on detecting patterns for every class of transaction. Nonetheless, the fact of altering the data lasts an ineffective way of fraud detection. For that reason, unsupervised learning is required to deal with data without altering it. The model using Autoencoder was therefore adopted. The latter (Autoencoder) proved a good performance in terms of classifying not fraud transactions as well as the fraud transaction with an f1-score of 93% (*Figure 4*(a,b)).



a. Confusion matrix of the model based on the Autoencoder architecture

	precision	recall	f1-score	support
0	0.99	1.00	0.99	986
1	1.00	0.87	0.93	97
accuracy			0.99	1083
macro avg	0.99	0.93	0.96	1083
weighted avg	0.99	0.99	0.99	1083

b. Classification report of the predictions made by the Autoencoder model

Figure 4: Results of Autoencoder

Based on an analysis study -which we have carried out depending on multiple metrics such as 'precision', 'recall', 'accuracy' and 'f1 score'- the findings indicate that Autoencoder has shown more effectiveness when compared to ANN and CNN. Nonetheless, our model still lacks immutability and traceability: two features ensuring safety, when we cope with the detection of non-legitimate credit card transactions. Concerning the first feature (immutability), it is needed in the sense that online operations may be changeable in the memory of our system after they occur; whereas our model can not ban this kind of modification. The second feature (traceability), means that our system can not identify nor measure the transaction throughout chained stages from the beginning until the ultimate point.

In the light of the findings comparing our study with the previous works in the same field, we deduce that our prototype is among the prior models -if not the only one- that show unpreceded robustness and efficiency embedded in the high scores generated after the training process arriving to 93% as f1 score in the classification case. Thus, a research contribution is added to the scope of detection and prevention of credit card fraud transactions.

5. CONCLUSION

In this work, we tried to target "Credit Card fraudulent transactions". It was -more or less -a successful attempt to decipher the complexity of this issue which is hidden in the absence of the dataset required to conduct such research, and dynamicity of fraudulent behaviors, sparsity of data, and class imbalance.

To designate effectively these challenges, we developed a model that achieved great results. Of course, thanks to several techniques we implemented during all the steps of implementation such as data sampling, feature selection, and boosting technique. All these strategies paved the way for our model to prove excellent performance in terms of classifying "not fraud" transactions as well as the "fraud" ones. Moreover, a new knowledge creation has been added to the field of credit card fraud detection, in the sense that immutability and traceability must be taken into consideration not only to detect fraudulent transactions but also to prevent them. Therefore, our research journey will not stop here but we are motivated to conduct another study, in which we will compare the efficiency of other unsupervised deep learning algorithms that might be more advanced to solve credit card fraud brain-teaser.

DATA AVAILABILITY

The data used to support the findings of this study are downloaded from Kaggle as mentioned above (section 3).

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

ACKNOWLEDGMENTS

We can not express enough gratitude to our supervisor, Mr. Mohammed Erritali, for his continuous guidance, support, and encouragement. We would like to thank profoundly everyone who helped us achieve this work.

REFERENCES

[1] Y. Kültür and M. U. Ça\uglayan, "Hybrid approaches for detecting credit card fraud," *Expert Syst.*, vol. 34, no. 2, p. e12191, 2017.

[2] D. Ge, J. Gu, S. Chang, and J. Cai, "Credit card fraud detection using lightgbm model," in *2020 international conference on E-commerce and internet technology (ECIT)*, 2020, pp. 232–236.

[3] A. Seetharaman, M. Senthilvelmurugan, and R. Periyanayagam, "Anatomy of computer accounting frauds," *Manag. Audit. J.*, 2004.

[4] J. Mackevičius and E. Ragauskien\.e, "Anatomy of frauds. Types, conditions, prevention measures," *Ekonomia*, vol. 14, p. 204, 2011.

[5] T. P. Bhatla, V. Prabhu, and A. Dua, "Understanding credit card frauds," *Cards Bus. Rev.*, vol. 1, no. 6, pp. 1–15, 2003.

[6] S. B. E. Raj and A. A. Portia, "Analysis on credit card fraud detection methods," in *2011 International Conference on Computer, Communication and Electrical Technology (ICCCET)*, 2011, pp. 152–156.

[7] E. L. Paula, M. Ladeira, R. N. Carvalho, and T. Marzagao, "Deep learning anomaly detection as support fraud investigation in brazilian exports and anti-money laundering," in *2016 15th ieee international conference on machine learning and applications (icmla)*, 2016, pp. 954–960.

[8] J. E. Turner, *Money laundering prevention: Deterring, detecting, and resolving financial fraud*. John Wiley \& Sons, 2011.

[9] A. T. Carswell and D. C. Bachtel, "Mortgage fraud: A risk factor analysis of affected communities," *Crime, law Soc. Chang.*, vol. 52, no. 4, pp. 347–364, 2009.

[10] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decis. Support Syst.*, vol. 50, no. 3, pp. 602–613, 2011.

[11] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed data mining in credit card fraud detection," *IEEE Intell. Syst. Their Appl.*, vol. 14, no. 6, pp. 67–74, 1999.

[12] S. Lakshmi and S. D. Kavilla, "Machine learning for credit card fraud detection system," *Int. J. Appl. Eng. Res.*, vol. 13, no. 24, pp. 16819–16824, 2018.

[13] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. (2018 Beling, "April). Deep learning detecting fraud in credit card transactions," *InSystems Inf. Eng. Des. Symp. (p*, pp. 129–134, 2018.

[14] A. Mishra and C. Ghorpade, "Credit card fraud detection on the skewed data using various classification and ensemble techniques," in *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2018, pp. 1–5.

[15] I. Benchaji, S. Douzi, and B. El Ouahidi, "Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection," in *International Conference on Advanced Information Technology, Services and Systems*, 2018, pp. 220–229.

[16] A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 1, pp. 18–25, 2018.

[17] N. Malini and M. (2017 Pushpa, "February). Analysis on credit card fraud identification techniques based on KNN and outlier detection," in *Inthird international conference on advances in electrical*, 2017, pp. 255–258.

[18] S. Dhankhad, E. Mohammed, and B. (2018 Far, "July)," in *Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study*, 2018, pp. 122–125.

[19] J. O. Awoyemi, A. O. Adetunmbi, and S. A. (2017 Oluwadare, "October)," in *Credit card fraud detection using machine learning techniques: A comparative analysis*, 2017, pp. 1–9.

[20] R. R. Popat and J. Chaudhary, "A Survey on Credit Card Fraud Detection Using Machine Learning," *Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018*,

pp. 1120–1125, Nov. 2018, doi: 10.1109/ICOEI.2018.8553963.

[21] J. Hariharakrishnan and N. Bhalaji, "Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things," *J. ISMAC*, vol. 3, p. 2, 2021.

[22] J. Błaszczyński, de Almeida Filho, A. T., A. Matuszyk, M. Szel\kag, and R. Słowiński, "Auto loan fraud detection using dominance-based rough set approach versus machine learning methods," *Expert Syst. Appl.*, vol. 163, p. 11374, 2021.

[23] V. Patil and U. K. Lilhore, "A survey on different data mining & machine learning methods for credit card fraud detection," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 5, pp. 320–325, 2018.

[24] S. Shakya, L. N. Pulchowk, and S. Smys, "Anomalies detection in fog computing architectures using deep learning," *J. J. Trends Comput. Sci. Smart Technol.*, vol. 1, no. 2020, pp. 46–55, 2020.

[25] J. I. Z. Chen and K. L. Lai, "Deep convolution neural network model for credit-card fraud detection and alert," *J. Artif. Intell.*, vol. 3, p. 2, 2021.

[26] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A financial fraud detection model based on LSTM deep learning technique," *J. Appl. Secur. Res.*, vol. 15, no. 4, pp. 498–516, 2020.

[27] A. RB and S. K. KR, "Credit card fraud detection using artificial neural network," *Glob. Transitions Proc.*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltp.2021.01.006.

[28] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, p. 105124, Feb. 2020, doi: 10.1016/j.knosys.2019.105124.

[29] I. Al-Turaiki and N. Altwaijry, "A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection," *Big Data*, vol. 9, no. 3, p. 233, Jun. 2021, doi: 10.1089/BIG.2020.0263.

[30] H. Bandyopadhyay, "Introduction to Autoencoders [Types, Training, Applications]." https://www.v7labs.com/blog/autoencoders-guide (accessed May 10, 2022).

[31] J. Brownlee, "Failure of Classification Accuracy for Imbalanced Class Distributions," *Machine Learning Mastery*, 2020. https://machinelearningmastery.com/failure-of-accuracy-for-imbalanced-class-distributions/ (accessed May 10, 2022).