Journal of Emerging Computer Technologies
Research Article
Received: *2024-01-30* | ***Reviewing:*** *2024-02-01* & *2024-03-08*| ***Accepted:*** *2024-03-10* | ***Online:*** *2024-02-10* | ***Issue Date:*** *2023-12-31*
Doi: 10.57020/ject.1428146

Fraud Transaction Detection For Anti-Money Laundering Systems Based On Deep Learning

Jorge Felix Martínez Pazos
Xetid University of Informatics Science
Havana, Cuba
jorgefmp.mle@gmail.com
0009-0009-2477-8611

Jorge Gulín González
Center for Computational Mathematics Studies
University of Informatics Science
Havana, Cuba
jgulingonzalez@gmail.com
0000-0001-7912-2665

David Batard Lorenzo
Center for Computational Mathematics Studies
University of Informatics Science
Havana, Cuba
dbatardl@gmail.com
0009-0007-3555-2875

Jorge Alejandro Robaina Morales
Xetid University of Informatics Science
Havana, Cuba
jorgea.robaina.dev@gmail.com
0009-0000-5077-5718

Moises Miguel Rodríguez Álvarez
Department of Digital Systems
University of Informatics Science
Havana, Cuba
mrdguezalvz@gmail.com
0009-0001-4582-7875

***Abstract*— This study addresses the escalating problem of financial fraud, with a particular focus on credit card fraud, a phenomenon that has skyrocketed due to the increasing prevalence of online transactions. The research aims to strengthen anti-money laundering (AML) systems, thereby improving the detection and prevention of fraudulent transactions. For this study, a Dense Neural Network (DNN) has been developed to predict fraudulent transactions with efficiency and accuracy. The model is based on deep learning, and given the highly unbalanced nature of the dataset, balancing techniques were employed to mitigate the bias towards the minority class and improve performance. The DNN model demonstrated robust performance, generalizability, and reliability, achieving over 99% accuracy across training, validation, and test sets. This indicates the model's potential as a powerful tool in the ongoing fight against financial fraud. The results of this study could have significant implications for the financial sector, corporations, and governments, contributing to safer and more secure financial transactions.**

Keywords— AMLs, Deep Learning, Dense Neural Networks, Financial Fraud, Fraud Transaction Detection.

I. INTRODUCTION

The issue of financial fraud is becoming increasingly prevalent, with far-reaching implications for the finance sector, businesses, and governments. One particular area of concern is credit card fraud, which has seen a rise in incidence due to the growing popularity of online transactions. Credit card fraud can be classified into two categories: internal fraud, which involves collaboration between cardholders and banks using false identities, and external fraud, which involves the use of stolen credit cards. Traditional methods for detecting fraudulent transactions are often slow and ineffective. As such, financial institutions are now turning to computational approaches to tackle the problem of credit card fraud [1].

In the contemporary era, marked by significant scientific and technological advancements, financial and banking institutions have increasingly turned to Anti-Money Laundering Systems (AMLs). AMLs serve as a robust line of defense against illicit activities such as money laundering and terrorist financing, which pose substantial threats to the integrity of financial systems and the broader economy. The adoption of AMLs by financial institutions is driven by the need to comply with stringent regulatory requirements, protect customer data, and maintain the reputation of the institution. AMLs employ sophisticated algorithms and machine learning techniques to monitor transactions and user activities, identify suspicious patterns, and generate alerts for further investigation. The effectiveness of AMLs is enhanced by the integration of various components that work in synergy to provide a comprehensive and robust approach to detecting and preventing fraudulent transactions [2].

The first line of defense in AML is transaction monitoring, which involves the active tracking and analysis of financial transactions. This process, which can be performed in real-time or periodically, is designed to identify and prevent fraudulent or illegal activity. As technology advances, transaction monitoring is becoming increasingly automated and relies on machine learning.

In parallel with transaction monitoring, user activity monitoring logs and tracks user actions on devices, networks, or websites. This component of AML is critical for detecting and stopping insider threats, whether accidental or malicious.

To further enhance the effectiveness of AMLs, rule-based approaches are used, which capture the knowledge of a human expert in a specialized domain and embody it in a computer system. The rules, encoded in the system as if-then-else statements, provide a structured way to analyze transactions and user activity.

Another key component of AMLs is graph analytics, which involves the study and manipulation of data structures that encapsulate relationships between entities. The analysis facilitates the identification of patterns, anomalies, and structures within relational data that can be critical in detecting money laundering patterns such as smurfing, ring, cascade, in-out, and direct star. Graph theory algorithms such as centrality detection, community detection, and node similarity allow knowledge to be extracted from transaction and user behavior. These algorithms provide insight into the importance of nodes

Cite (APA): Martínez Pazos, J.F., Gulín González, J., Batard Lorenzo, D., Robaina Morales, J.A., Rodríguez Álvarez, M.M. (2023). Fraud Transaction Detection For Anti-Money Laundering Systems Based On Deep Learning. *Journal of Emerging Computer Technologies*, 3(1), 29-34. Doi: 10.57020/ject.1428146

within the network (centrality), the clustering of similar nodes (community detection), and the similarity between nodes (node similarity).

Finally, Know Your Customer (KYC) and Know Your Business (KYB) processes are regulatory requirements that ensure companies are doing business with legitimate individuals and entities. KYC focuses on identifying individual customers, while KYB verifies the companies they do business with. Both processes are critical to preventing online fraud and financial crime and complying with anti-money laundering regulations.

The adoption of AMLs by financial and banking institutions represents a proactive and strategic response to the challenges posed by financial fraud and cyber threats. By leveraging advanced technologies and scientific knowledge, these institutions are better equipped to detect and prevent fraudulent transactions, thereby contributing to the security and stability of financial systems.

Several approaches have been used to detect fraudulent transactions. Machine learning based approaches have been intelligently used to detect fraudulent transactions by analyzing a large number of financial data. The most satisfactory machine learning techniques such as an ensemble of decision tree (EDT), and deep learning techniques such as stacked auto-encoders (SAE) and restricted Boltzmann machines (RBM) classifiers are applied to the preprocessed data [3]. Varmedia et al, 2019 and Xuan et al, 2018 employed supervised learning approaches, mainly Random Forest, Logistic Regression, and Gaussian Naive Bayes, for the task of fraud detection in transactions, while Dornadula & Geetha, 2019 applied a sliding window technique to the data, which allowed them to aggregate multiple transactions over time, thereby obtaining a greater amount of important information about transactions over time. On the other hand, Jhon & Nazz, 2019 and Zadafiya et al. 2022 used unsupervised learning methods, specifically local outlier factors, and isolation forests, for fraud detection. These approaches are particularly practical in scenarios where it is necessary to assign a score to a transaction to determine its level of anomaly.

The existing financial infrastructure within Cuba is currently devoid of a proactive, automated Anti-Money Laundering (AML) system. This deficiency underscores the necessity for an in-depth exploration and understanding of the operational mechanisms of AML systems. Consequently, this research endeavor is designed to illuminate these mechanisms and propose an innovative solution specifically tailored to enhance the transaction monitoring facet of an AML system. This proposed solution aims to bolster the efficiency and effectiveness of detecting and preventing illicit financial activities, thereby fortifying the integrity of Cuba's banking system.

The following encapsulates the key contributions that underscore the significance of the forthcoming study:

- The development of a robust model, grounded in Neural Networks, that achieves transaction classification with an accuracy exceeding 99%.
- The implementation of the Min Class Balance reaffirms the potential of balanced training sets for enhancing the robustness and generalizability of Machine Learning and Deep Learning models. This approach effectively mitigates biases towards the less-represented class.
- A comprehensive initial guide covering most components of Anti-Money Laundering (AML) systems, addressing the current lack of information and documentation provided by companies and organizations regarding these solutions.

II. Materials & Methods

A. Dataset

The study in question utilizes a dataset, sourced from Kaggle, that is pivotal in the exploration of credit card fraud. This dataset is employed to construct an Artificial Neural Network (ANN) with the aim of efficiently and accurately predicting fraudulent transactions based on the dataset's features [9].

The `distance_from_home` feature, which measures the distance from the cardholder's residence to the transaction location, could potentially flag anomalous activity if transactions consistently occur at locations significantly distant from the cardholder's habitual transaction sites. The `distance_from_last_transaction` feature calculates the spatial difference between the current transaction and the preceding one. A substantial shift in transaction locations could potentially serve as an indicator of fraudulent activity. The `ratio_to_median_purchase_price` feature, representing the ratio of the transaction's purchase price to the median purchase price, could suggest fraudulent activity if a transaction deviates significantly from the median. The `repeat_retailer` feature indicates whether the transaction was conducted with a retailer previously used by the cardholder. Regular transactions with the same retailer could suggest a trusted retailer or a potential point of compromise. The `used_chip` feature signifies whether the transaction was executed using a chip-enabled credit card. Transactions conducted using a chip are generally deemed more secure than those using a magnetic stripe. The `used_pin_number` feature denotes whether the transaction was authenticated using a PIN. Transactions verified using a PIN are typically considered more secure. The `online_order` feature indicates whether the transaction was conducted online. Online transactions could potentially be more susceptible to fraud if adequate security measures are not implemented. Finally, the `fraud` feature signifies whether the transaction was fraudulent. This is likely the target variable for predictive modeling [9].

Each of these features contributes to the comprehensive understanding of credit card fraud. By studying patterns and anomalies in these features, it may be possible to construct a model that can accurately predict fraudulent transactions, thereby helping to mitigate the impact of credit card fraud. The insights derived from this analysis could be instrumental in enhancing the security measures employed by financial institutions and fostering a safer transaction environment for consumers. This study exemplifies the potential of machine learning in enhancing the security and reliability of financial systems and institutions.

B. Exploratory Data Analysis

The dataset under investigation, titled "Credit Card Fraud," comprises one million tuples and exhibits a significant imbalance, as illustrated in Figure 1. This imbalance is primarily due to the overwhelm-ing prevalence of genuine transactions compared to fraudulent ones. Such a disparity in class distribution poses unique challenges in model development, as the model must be sensitive enough to accurately identify the minority class (fraudulent transactions) without being overwhelmed by the majority class (genuine transactions). This aspect underscores the complexity of fraud detection in credit card transactions and highlights the need for sophisticated modeling techniques to effectively tackle this issue. The dataset initially contains 912,597 instances of genuine transactions and 87,403 instances of fraudulent transactions. However, to combat biases and enhance the model's performance and generalizability, a class balance is performed. This process adjusts the dataset so that genuine transactions constitute 60% of the total data and fraudulent transactions make up the remaining 40%. This approach ensures a better balance between the classes, which is crucial in machine learning models to prevent overfitting to the majority class and improve the detection of the minority class.

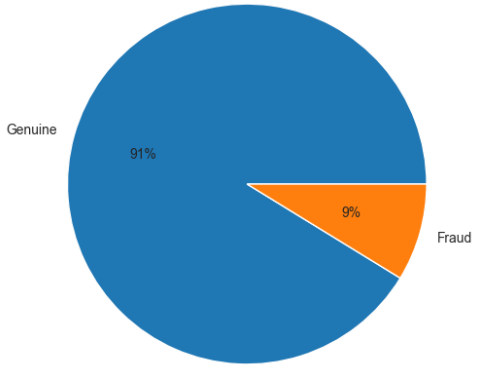

Figure 1. Pie chart of the dataset classes distribution

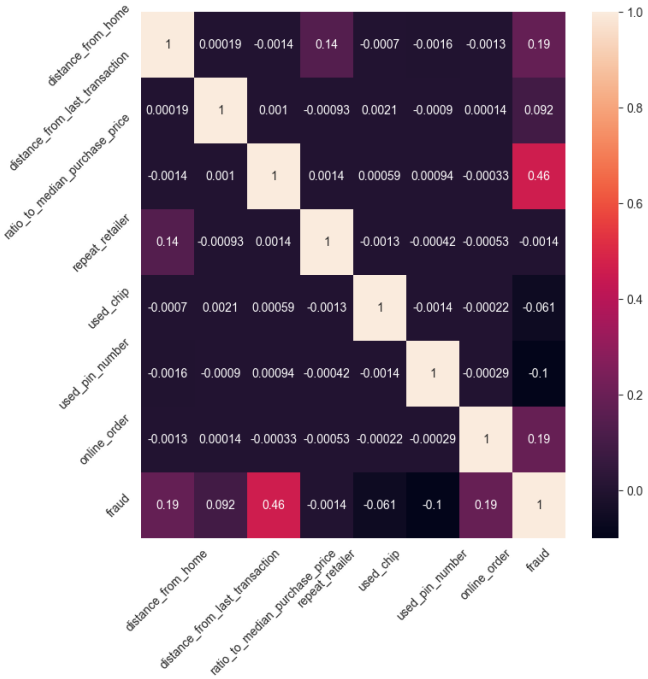

Figure 2: Correlational heatmap of the dataset attributes

As delineated in the correlational heatmap in figure 2, the feature most strongly correlated with whether a transaction is fraudulent is `ra-tio_to_median_price_purchase`. Despite this, other features such as `distance_from_home` and `online_order` exhibit a lesser degree of correlation. It's important to note that while these features may be less correlated, they still contribute valuable information that can enhance the predictive power of a model. In the complex landscape of fraud detection, even features with minor correlations can play a significant role when combined with other data points. Therefore, a comprehensive approach that considers a wide range of features is often most effective in accurately identifying fraudulent transactions.

C. Model Building & Training

Following the comprehensive data preprocessing and exploratory data analysis outlined above, the dataset has been partitioned into three distinct sub-sets: 70% for training, 15% for validation, and 15% for testing. This partitioning strategy facilitates the evaluation of the model's performance upon the completion of the training process.

The Dense Neural Network architecture designed for detecting fraud in transactions is constructed using TensorFlow's Keras API. This model is sequential, meaning that the layers are stacked linearly. The architecture begins with a dense layer with 64 neurons and a Rectified Linear Unit (ReLU) activation function. The input shape corresponds to the number of features in the training data (None, 7). The ReLU activation function is used to introduce non-linearity into the model, allowing it to learn more complex patterns. Following the first dense layer, a dropout layer is applied with a rate of 0.2. Dropout is a regularization technique that helps prevent overfitting by randomly setting a fraction of input units to 0 during training, which helps the model to generalize better to unseen data. The next layer is another dense layer with 32 neurons, again using a ReLU activation function. This is followed by another dropout layer with a rate of 0.2. The model then includes a third dense layer with 16 neurons and a ReLU activation function, followed by a dropout layer with a higher rate of 0.4. This increased dropout rate may help to further regularize the model and reduce overfitting. Next, a batch normalization layer is included. Batch normalization is a technique to provide any layer in a neural network with inputs that have zero mean/unit variance, which aids in overall network training [10], [11]. Finally, the architecture concludes with a dense output layer with 2 neurons, corresponding to the two classes (fraudulent and genuine transactions). The softmax activation function is used in this layer to output a probability distribution over the two classes, meaning the output can be interpreted as the model's confidence that the transaction is fraudulent or genuine.

The model is compiled with the Adam optimizer with a learning rate of 3e-4 and the sparse categorical cross-entropy loss function. The Adam optimizer is an adaptive learning rate optimization algorithm that's been designed specifically for training deep neural networks. The sparse categorical cross-entropy loss is suitable for multi-class classification problems. The metric used to evaluate the model during training is accuracy. The subsequent figure 3 provides a graphical

representation of the Dense Neural Network architecture, illustrating input flow and output flow.

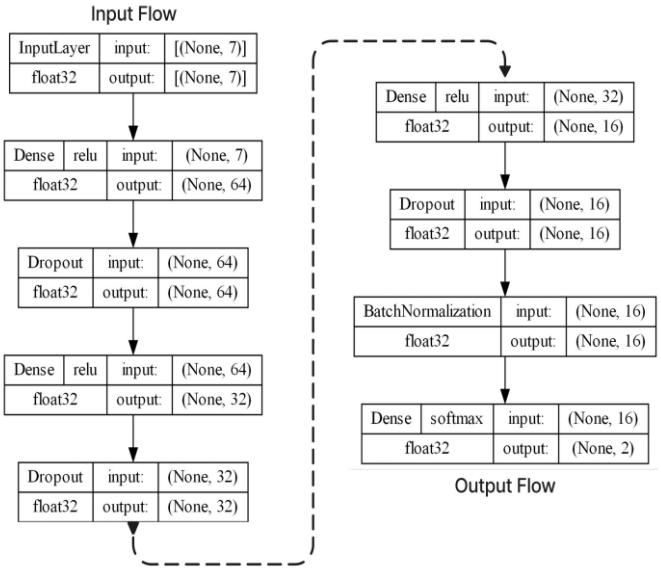

Figure 3. Architecture of the proposed Dense Neural Network model.

The model is trained using two specific callback functions: Early Stopping and Learning Rate Reduction. The Early Stopping callback is implemented to halt the training process when a monitored metric, in this case, validation accuracy, ceases to improve. The patience parameter is set to 10, indicating that the training will be stopped if there is no improvement in the validation accuracy after 10 epochs. The restore best weights parameter is set to True, ensuring that the model weights from the epoch with the optimal monitored metric are restored. The Learning Rate Reduction callback is utilized to reduce the learning rate when a metric has stopped improving. The metric monitored here is also the validation accuracy. The patience parameter is set to 4, denoting that if the validation accuracy does not improve after 4 epochs, the learning rate will be reduced. The factor parameter is set to 0.8, indicating that the learning rate will be reduced by a factor of 0.8. The min lr parameter is set to 0.000001, establishing the lower bound for the learning rate.

The model is then trained for a maximum of 150 epochs with a batch size of 1024, and using the validation set. The training process utilizes both the Early Stopping and Learning Rate Reduction callbacks [12]. This approach to training allows for a more efficient search for model parameters and can lead to improved model performance.

III. Results & Discussions

The model history of the implemented Dense Neural Network for fraud detection which is shown in Figure 4, offers an in-depth perspective on the model's learning progression and performance. The graphs depicting "Training & Validation Loss" and "Training & Validation Accuracy" collectively suggest that the model is effectively assimilating knowledge from the training data and demonstrating robust generalization capabilities when applied to unseen data in the validation set. This is substantiated by the consistent decrease in loss and increase in accuracy over time for both the training and validation sets, culminating in a training accuracy of 99.3%, validation accuracy of 99.7%, loss of 0.0202, and validation loss of 0.0075 at epoch 69. The near-perfect alignment of the loss and validation loss lines further indicates that the gradient is consistently moving toward an improved state.

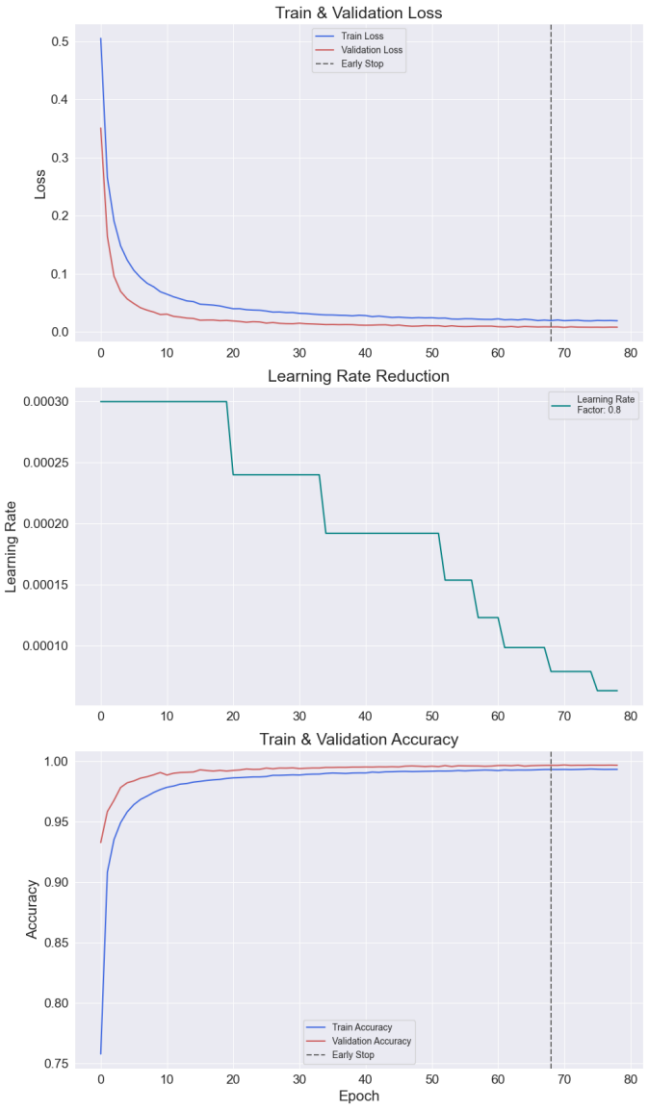

Figure 4. Model history of the proposed Dense Neural Network

The evaluation of predictive models on unseen data is of paramount importance to ascertain their per-formance in real-world scenarios. Without a com-prehensive evaluation on data that was not part of the training process, there exists a risk of sub-optimal real-world performance, potentially leading to erroneous decision-making. By subjecting the model to evaluation with novel data, a more accu-rate understanding of its real-world performance can be gleaned, thereby bolstering confidence in its deployment and ensuring its reliability and safety for integration into real-world solutions.

In the context of the Dense Neural Network model for fraud detection, the classification report provides a detailed account of its performance metrics [13]. The model exhibits a high degree of precision and recall for both ‘Fraud’ and ‘Not Fraud’ classes, with values exceeding 99% in all cases. Specifical-ly, the ‘Not Fraud’ class has a precision of 99.8% and a recall of 99.6%, resulting in an F1-score of 99.7%. Similarly, the ‘Fraud’ class has a precision of 99.4% and a

recall of 99.7%, leading to an F1-score of 99.6%. The overall accuracy of the model is 99.7%, with the macro and weighted averages for precision, recall, and F1-score all being 99.7%.

These results indicate that the model demonstrates a high level of effectiveness in distinguishing be-tween 'Fraud' and 'Not Fraud' instances. The high precision suggests that the model has a low false positive rate, while the high recall indicates a low false negative rate. The F1-score, being the harmonic mean of precision and recall, further confirms the model's robust performance. This comprehensive evaluation underscores the model's potential for reliable and safe deployment in real-world fraud detection solutions. Table 1 summarizes the classification report of the proposed Dense Neural Network.

Table 1: Summary of the classification report

	precision	recall	f1-score
Not Fraud	99.8	99.6	99.7
Fraud	99.4	99.7	99.6
Accuracy	99.7	99.7	99.7
Macro AVG	99.6	99.7	99.7
Weighted AVG	99.7	99.7	99.7

This confusion matrix provides a granular view of the model's performance. As detailed in Figure 5, the model correctly classified 19654 instances as Not Fraud and 13017 instances as Fraud. However, there were 72 instances where the model incorrectly classified 'Not Fraud' instances as 'Fraud' (False Positives) and 33 instances where 'Fraud' was incorrectly classified as 'Not Fraud' (False Negatives) [14].

The minimal number of false positives and false negatives suggests that the model has high precision and recall, confirming the metrics observed in the classification report. This further emphasizes the robust performance of the model in fraud detection, underscoring its potential for reliable use in real-world applications.

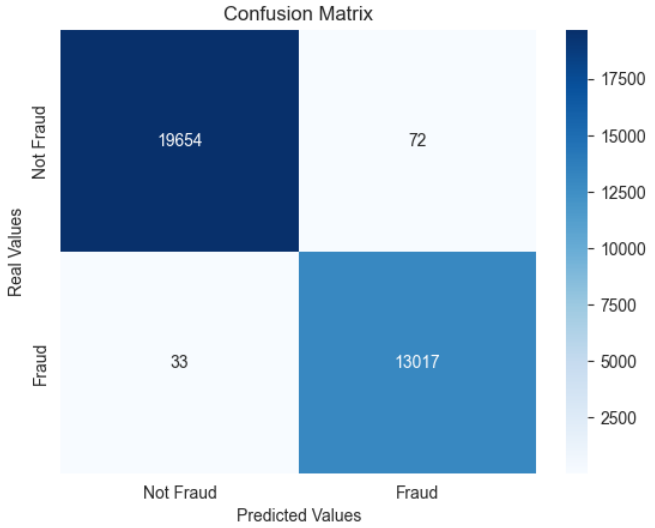

Figure 5. Confusion matrix of the model evaluation over the test set.

The AUC (Area Under the Curve) score and the ROC (Receiver Operating Characteristic) curve are critical metrics for evaluating the performance of a binary classification model. The AUC score for this model is 0.997, which is remarkably close to 1. This indicates that the model has a high measure of separability and is highly capable of distinguishing between positive and negative classes. The ROC curve, which is a plot of the true positive rate against the false positive rate, provides a visual representation of the model's performance across all thresholds. The curve for this model appears to be close to the ideal top-left corner of the plot, suggesting a high true positive rate and a low false positive rate. The previous description is detailed in Figure 6 [15].

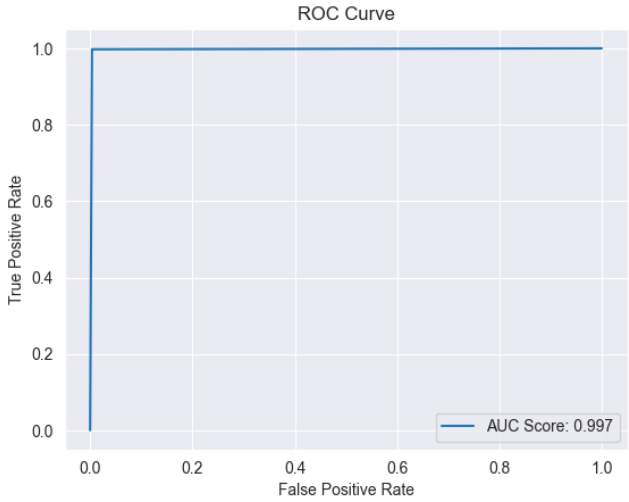

Figure 6. ROC Curve of the model evaluation over the test set

The Dense Neural Network model proposed in this research for fraud detection represents a significant contribution to the financial sector and cyber-security. Its high performance, as evidenced by the AUC score and the confusion matrix, demonstrates its robust ability to accurately distinguish between fraudulent and non-fraudulent transactions. This accuracy is paramount in the financial sector, where the timely detection and prevention of fraudulent activities can result in substantial cost savings and enhance the security of financial transactions.

Table 2. Comparative analysis of model performance in the literature.

Model	Accuracy (%)	Precision (%)	Recall (%)	Learning Type
Varmedja et al [4]: LR	97.46	58.82	91.84	Supervised
Varmedja et al [4]: NB	99.23	16.17	82.65	Supervised
Varmedja et al [4]: RF	99.96	96.38	81.63	Supervised
Varmedja et al [4]: MLP	99.93	79.21	81.63	Supervised
Xuan et al [5]	98.67	32.68	59.62	Supervised
Dornadula et al [6] RF	99.9	**99.9**	-	Supervised
Jhon & Naaz [7] LOF	97	-	-	Unsupervised
Jhon & Naaz [7] IF	71	-	-	Unsupervised
Zadafiya et al [8] IF	**100**	65	64	Unsupervised
Zadafiya et al [8] IF	**100**	51	51	Unsupervised
Proposed DNN Model	99.7	99.6	**99.7**	Supervised

The comparison delineated in Table 2 involves models that utilize distinct datasets for their training and evaluation processes. In this table, values are emphasized in bold to

indicate superior performance, however, it should be noted that in the studies conducted by Dornadula et al. [6], the recall metrics were not evaluated, similarly, in the research undertaken by John and Naaz [7], neither precision nor recall was assessed. Despite other models outperforming the proposed model in certain metrics, the proposed model generally exhibits superior performance across all metrics in the comparison. The model from the Dornadula et al [6] study emerges as the most competitive against the proposed model in terms of accuracy and precision, although a comparison of recall metrics is not possible.

In the realm of cybersecurity, the model's ability to detect anomalies and classify transactions with high precision contributes to the strengthening of security protocols. By identifying potential threats, it aids in the proactive mitigation of cyber risks, thereby enhancing the overall security posture of financial institutions. Furthermore, the adaptability of the model allows for its integration into the existing infrastructure of any financial institution or bank. By training the model on institution-specific data, it can be tailored to detect fraud patterns unique to the institution, thereby increasing its effectiveness.

The model can be integrated as an AI monitoring component into a real-time Anti-Money Laundering (AML) system. Utilizing technologies such as Kafka and PySpark for data sourcing and streaming, the model can analyze and classify transactions in real time. This not only allows for immediate detection and response to fraudulent activities but also enables continuous learning and adaptation to evolving fraud patterns.

IV. Conclusions

While acknowledging that an Anti-Money Laundering system consists of more components than just AI monitoring, the focus of this paper has been on the development and evaluation of an AI model for transaction fraud detection based on deep learning.

The proposed model, a dense neural network, has exhibited exceptional performance, with precision, recall metrics, and an Area Under the Curve score all approximating 99.7%. The model's robustness is further underscored by its use of a class balance method, ensuring an unbiased generalization capability. Comparative analysis with extant models reveals that the proposed model generally outperforms on key performance metrics. Its architecture is designed for seamless adaptability and integration into pre-existing financial systems, thereby bolstering the security of financial transactions and the integrity of the financial system at large. This research represents an important milestone and lays a solid foundation for future research and implementation of an anti-money laundering system specifically tailored to the Cuban banking sector, which currently lacks a proactive system of this type.

References

[1] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI). http://dx.doi.org/10.1109/ICCNI.2017.8123782

[2] Narayan, A., Kumar, S. D. M., & Chacko, A. M. (2023). A Review of Financial Fraud Detection in E-Commerce Using Machine Learning. First Online: 24 February 2023. 346 Accesses. Conference paper. http://dx.doi.org/10.1007/978-981-19-7524-0_21

[3] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., et al. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences, 12(19), 9637. MDPI AG. http://dx.doi.org/10.3390/app12199637

[4] Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019). Credit Card Fraud Detection - Machine Learning methods. 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH). https://doi.org/10.1109/infoteh.2019.8717766

[5] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018). Random forest for credit card fraud detection. 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). https://doi.org/10.1109/icnsc.2018.8361343

[6] Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. Procedia Computer Science, 165, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

[7] John, H., & Naaz, S. (2019). Credit card fraud detection using local outlier factor and isolation forest. Int. J. Comput. Sci. Eng, 7(4), 1060-1064.

[8] Zadafiya, N., Karasariya, J., Kanani, P., & Nayak, A. (2022). Detecting Credit Card Frauds Using Isolation Forest And Local Outlier Factor-Analytical Insights. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1588-1594). IEEE

[9] Narayanan R, D. (2021). Credit Card Fraud. Kaggle. Available at: https://www.kaggle.com/datasets/dhanushnarayananr/credit-card-fraud

[10] Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. R. (2012). Improving neural networks by preventing co-adaptation of feature detectors. arXiv preprint arXiv:1207.0580. https://doi.org/10.48550/arXiv.1207.0580

[11] Ioffe, S., & Szegedy, C. (2015, June). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In International conference on machine learning (pp. 448-456). pmlr. https://doi.org/10.48550/arXiv.1502.03167

[12] Keras. Keras API Reference. Available online: https://keras.io/api. Last Accessed 28/3/2023

[13] Scikit-learn. (2023). Classification Report. Available at https://scikit-learn.org/stable.

[14] Ting, K.M. (2011). Confusion Matrix. In: Sammut, C., Webb, G.I. (eds) Encyclopedia of Machine Learning. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-30164-8_157

[15] Hoo, Z.H., Candlish, J., Teare, D., (2017). What is a ROC curve?. Emergency Medicine Journal 34, 357–359.. https://doi.org/10.1136/emermed-2017-206735