Research Article Journal of Contemporary Education Theory & Artificial Intelligence

Enhancing Performance of Financial Fraud Detection Through Machine Learning Model

Authors:

Eswar Prasad Galla^{1*}, Hemanth Kumar Gollangi², Venkata Nagesh Boddapati³, Manikanth Sarisa⁴, Kiran Polimetla⁵, Shravan Kumar Rajaram⁶, Mohit Surender Reddy⁷

¹Department of Computer Science, University of Central Missouri. Email: Gallaeswar43@gmail.com ²Department of Computer Science, Missouri State University. Email: hemanthkumargollangi19@gmail.com

³Microsoft, Support Escalation Engineer. Email: VenkataNagesh.boddapati@student.ctuonline.edu

⁴Principal Software Engineer, Ally Financial Inc. Email: Mk2703@outlook.com

⁵Adobe Inc, Software Engineer. Email: Kiran.polimetla@gmail.com

⁶Microsoft, Support Escalation Engineer. Email: Shravankumar.rajaram@gmail.com

⁷Microsoft, Support Escalation Engineer. Email: mohitreddy17@gmail.com

*Corresponding author: Eswar Prasad Galla, Department of Computer Science, University of Central Missouri

Citation: Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

Received Date: 10 October, 2023; Accepted Date: 18 October, 2023; Published Date: 23 October, 2023

Abstract

Despite attempts to reduce it, financial fraud continues to be a major problem in many industries, including healthcare, banking, and insurance. Traditional fraud detection techniques, which are often manual, are inefficient, time-consuming, and costly. As a result, methods that use AI and ML have been implemented to improve fraud detection procedures. This study examines the application of ML algorithms for credit card fraud detection using a dataset consisting of 284,807 transactions made by European cardholders in 2013, out of which 492 were fraudulent. Preprocessing steps, including Label Encoding, SMOTE for handling class imbalance, and PCA for feature reduction, were applied to the dataset. On the training dataset have applied ML based classification models like DT, SVM, and ANNs were employed to evaluate their performance. The models were assessed using accuracy, precision, and recall as key metrics. The ANN model emerged as the best-performing model, achieving 98.41% precision, 98.69% accuracy, and 98.98% recall, outperforming both Decision Trees and SVM. This study highlights the effectiveness of ML models, particularly ANNs, in improving financial fraud detection.

Keywords: Financial Fraud, Machine Learning, Credit Card Transaction Dataset, Detection.

Introduction

Financial fraud refers to the practice of acquiring money using deceitful and illegal methods. Many different types of businesses, banks, insurance companies, and government agencies are vulnerable to financial fraud [1]. Crimes against the financial system, such as money laundering and fraudulent financial transactions, have become more problematic for many industries and companies in recent years. Financial fraud continues to have a detrimental influence on society and the economy despite many efforts to reduce it. Every day, large amounts of money are wasted due to this crime [2]. A variety of methods for detecting fraud were developed long ago. Not only is physical labour required for most traditional operations, but it is also inefficient, costly, and prone to error. Despite their ineffectiveness, more research is being conducted to mitigate costs caused by fraudulent activities. The advancement of AI has allowed for the use of data mining and ML to detect fraudulent activities in the financial sector. Both supervised and uncontrolled methods were used to anticipate fraud acts. Classification is the gold standard method for detecting financial fraud[3].

ML is a branch of AI that enables machines to draw conclusions from past data by examining patterns. With Google DeepMind's phenomenal achievement in 2015, AI and ML have reached new heights[4]. A few real-world applications of deep anomaly detection include security breach detection in computer networks, fraud detection in healthcare, banking, insurance, and mobile cellular networks, detection of anomalies in medical and malware, and detection of anomalies in video surveillance. ML has many uses in the IoT realm, including location monitoring, detecting Android malware, automating the house, and forecasting the incidence of heart disease[5].

This project aims to investigate and evaluate ML methods for identifying instances of financial transaction fraud, with a specific emphasis on credit card fraud. With the rise of financial fraud, traditional methods of detection, which are often manual, have proven to be time-consuming, costly, and inefficient. By leveraging machine learning models, the study aims to identify approaches that can effectively and accurately detect fraudulent transactions. The objective of this study is to enhance financial sector fraud detection systems and reduce economic losses by comparing several models, such as DT, NB, and ANN, and highlighting the advantages and disadvantages of each approach. The following are the main contribution of the study on financial fraud detection based on Credit card transaction dataset:

- By comparing models like DT, NB, and ANNs, the study identifies the most effective techniques for fraud detection based on key metrics like recall, precision, and accuracy.
- The study applies its analysis on a real-world credit card transaction dataset, which adds practical relevance to its

findings on model performance and effectiveness in detecting fraudulent activities.

- It demonstrates how preprocessing techniques like SMOTE for handling class imbalance and PCA for feature reduction can improve model performance in fraud detection.
- The study shows that Artificial Neural Networks (ANNs) outperform other models according to accuracy, precision, and recall, making it a highly effective technique for financial fraud detection.

Structure of the paper

This research is organised in the following way: Predicting online sales is the focus of Section 2, which summarises current approaches. The approach, including data management and model application, is described in Section 3. The outcomes of the experiments are detailed and discussed in Section 4. Section 5 presents the important findings and suggests areas for further research.

Literature Review

This section reviews key machine learning research on similar datasets and challenges, highlighting influential methods and studies. Table 1 summarizes the relevant literature for financial fraud detection.

This paper Rai and Dwivedi, (2020), proposes a way to detect fraudulent activity in credit card data by using a NN based unsupervised learning methodology. This new approach outperforms the state-of-the-art AE, LOF, IF, and K-Means clustering algorithms. In comparison to the existing approaches, which include AE, IF, LOF, and K Means, the proposed NN-based fraud detection system achieves an accuracy of 99.87% [6].

This study Hidayattullah, Surjandari and Laoh, (2020), uses a variety of ML methods grounded on meta-heuristic optimisation to construct reliable financial statement fraud prediction models. Two different types of classification algorithms were employed: SVMs and Back Propagation Neural Networks. This study's top classifier is a SVM, with 96.15% accuracy achieved by optimising its parameters using a Genetic Algorithm [7].

This paper Mubalaike and Adali, (2018), seeks to comprehend the ways in which DL models may be helpful in accurately identifying fraudulent transactions. The preprocessed data is then subjected to the best ML and DL methods, including ensembles of decision trees (EDTs) and SAEs and RBM classifiers. An optimum accuracy value are 90.49%, 80.52%, and 90.49%, respectively. A closer look at the findings shows that RBM outperforms the alternatives [8].

This study Gardner et al. (2019), stress the need of creating a system that can identify anomalies in financial transactions using three different components. In order to build the system, many RFC with distinct fitness functions are fine-tuned. By optimising the RF parameters to meet the fitness function, the procedure is carried out using a randomised grid search. When all of the models are finished, they are compared to create three levels of discovered frauds, with varying degrees of accuracy in each level. Detected frauds may be categorised into multiple levels for improved recall and precision. Using this method, we are able to accurately classify 96% of frauds while detecting

85% with an accuracy of above 90%. According to our research, the tiered random forest achieves a recall of 72% and a precision of 85%, making it the most effective algorithm compared to SVM and logistic regression [9].

In this paper Erfani, Shoeleh and Ghorbani, (2020), provide a streamlined system for identifying fraudulent activities. In order to identify fraud, our methodology employs deep support vector data description after a unique preprocessing and subsampling phase. They offer a trend analysis that takes into account the dimensions of the training and test datasets as well as the model's performance as measured by ROC-AUC and AP. Last but not least, our method beats the advance binary classifiers, RF and SVM, in several tests. The best values are 90% for AP and 93% for ROC-AUC, demonstrating its outstanding performance [10].

This paper Arun and Venkatachalapathy, (2020), announces a new C-LSTM model for detecting credit fraud that is based on DL. Two steps are involved in the suggested C-LSTM model: preprocessing and classification. Using a German Credit and Kaggle's CCFD datasets, we verify a performance of a C-LSTM model. The obtained experimental outcomes demonstrated that, when applied to a German credit and CCFD dataset, the C-LSTM model performed well with accuracy of 94% and 94.65% [11].

Table 1: Comparative research of Financial Fraud
Detection using machine and deep learning techniques

Ref	Methodolog	Datase	Result	Limitation and	
	y	t		future work	
[1]	Neural	Credit	99.87%	May not	
	Network	card	accurac	generalize to	
	(NN) based	data	у	different types	
	unsupervised			of fraud or data	
	learning			variations	
	technique				
[2]	Meta-	Financ	SVM	May be limited	
	heuristic	ial	with	by the quality	
	optimization	statem	Genetic	and	
	with Back	ents	Algorit	representativene	
	Propagation		hm:	ss of financial	
	Neural		96.15%	data used	
	Networks		accurac		
	and SVM		у		
[3]	Ensemble of	One	EDT:	Performance	
	Decision	month	90.49%,	might vary with	
	Tree (EDT),	of	SAE:	different	
	Stacked	financi	80.52%,	datasets and the	
	Auto-	al logs	RBM:	extensive	
	Encoders	from a	91.53%	computation	
	(SAE), RBM	mobile		required	
		money			
		service			
[4]	Three-tiered	Not	96%	High	
	anomaly	specifi	correct	complexity of	
	detection	ed	fraud	tuning and	
	system with		classific	parameter	
	randomized		ation;	optimization;	
	grid search		Precisio	may not scale	
	and multiple		n over	well	

	Random		90% for	
	Forest		85% of	
	classifiers		detected	
			frauds	
[5]	Preprocessin	Not	AP:	Framework's
	g and	specifi	90%,	performance
	subsampling	ed	ROC-	might depend
	with Deep		AUC:	on the specifics
	Support		93%	of preprocessing
	Vector Data			and
	Description			subsampling
				steps
[6]	C-LSTM	Germa	German	May require
	model	n	Credit:	substantial
		Credit	94%,	computational
		dataset	Kaggle	resources and
		,	Credit	may not handle
		Kaggle	Card	all fraud types
		Credit	Fraud	equally
		Card	Detecti	
		Fraud	on:	
		Detecti	94.65%	
		on		
		dataset		

Research gaps

While existing studies on fraud detection have demonstrated significant advancements with various methodologies—such as NN-based unsupervised learning, meta-heuristic optimization, and deep learning techniques—there remains a notable research gap in generalizing these methods across diverse datasets and real-world scenarios. Many approaches are optimized for specific datasets, such as mobile money transactions or financial statements, limiting their applicability to broader contexts. Additionally, the complexity of tuning and preprocessing methods, along with the variability in performance metrics like accuracy and precision, indicates a need for more robust and adaptable frameworks. Future research should focus on developing universal models that integrate advanced techniques and improve generalization, while also addressing the resource-intensive nature of current optimization processes.

Research Methodology

In this research aim to provide the efficient ML based financial fraud detection system. Beginning with the gathering of a dataset consisting of 284,807 transactions by European cards, including 492 instances of fraud, the technique for evaluating this information for the purpose of detecting fraud uses a structured approach. The data is carefully prepared for analysis by filling in missing values, eliminating duplicates, standardising it, and encoding categorical variables employing Label Encoding. Using SMOTE and PCA for feature selection helps with class imbalance. The dataset is then divided into training (80%) and testing (20%) subsets. An assortment of classification models, such as DT, NB, and ANNs, are tested and assessed for their accuracy and efficacy in differentiating between genuine and fraudulent transactions. Figure 1 shows a flow diagram of the system that detects financial fraud.

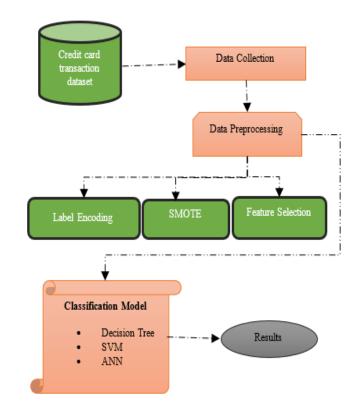


Figure 1: Proposed flowchart of financial fraud detection system.

A following data flowchart of financial fraud detection system steps are listed, shows in figure 1. Each level of data processing in the system is explained in depth.

1) Data collection

The process of data collection involves collecting relevant information from many sources, such as sensors and databases, in order to construct a large and representative dataset for analysis. There is a notable disparity between the 284,807 credit card transactions recorded for European cardholders in September 2013 and the 492 fraudulent transactions.

2) Data preprocessing

The term "data processing" refers to the steps used to make raw data more suitable for analysis. This includes resolving missing data, removing duplicates, and encoding category variables. Data preparation for modelling involves checking for quality and consistency in order to boost the efficiency of later analyses and ML algorithms. Here are some of the most important preprocessing steps:

- Label Encoding: Label Encoding is a way to make numerical values out of category data. Algorithms that work with numerical input can handle categorical data since each category is given its own distinct integer.
- **SMOTE:** The SMOTE, which generates synthetic samples for the minority class, is one way to remedy class imbalance. By interpolating between preexisting data points, it generates additional, synthetic data points, hence enhancing the performance of ML models on unbalanced datasets.
- Feature Selection: Principle Component Analysis converts a dataset's characteristics into a new collection of variables known as principle components, therefore lowering a number of features in the dataset. These elements capture the majority of the volatility in the data, enabling a more condensed depiction without sacrificing crucial details.

Citation: Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

3) Data Splitting

A potential solution to address class imbalance is the SMOTE, which creates synthetic samples for the minority class. The effectiveness of ML models on imbalanced datasets is improved by interpolating between extant data points to create new, synthetic data points. The model will be trained using 80% of the data and tested with 20%. This ratio is intended to ensure that a smaller sample size is used for testing once the model has been trained on the majority of the data.

4) Classification Models

This section describes how the Credit Card Transaction dataset was analysed using several categorisation techniques. These models are used to assess and compare their performance across the provided features. The goal of this analysis is to find the model that provides the most insightful and accurate findings when applied to product ratings and customer reviews.

a) Decision Tree

Regression and classification problems are two of the most common and extensively utilised supervised ML techniques that are available: decision trees. The Decision Tree method has a simple yet very effective intuition. Classifying non-linearly separable data is possible with little effort spent training the algorithm. When contrasted with KNN and other classification algorithms, it demonstrates remarkable speed and efficiency. The two most used metrics for selecting attributes are entropy and information gain.

b) SVM

SVMs are another well-liked supervised learning for classification method. This classifier uses a hyper plane to divide the dataset into categories; it's discriminative. One way to divide up n-dimensional data is via a hyper plane. A hyper plane that maximises the margin is chosen from among numerous possible separations of the dataset. When compared to other algorithms, SVM uses less processing time while yet providing good accuracy.

c) ANN

The three layers that make up an ANN are an input, hidden, and output layers. An input layer is responsible for supplying the neural network with input information; a hidden layer is a brain of a network, constantly updating the weights to improve performance; and an output layer is where a network's results are rendered in class terms. The propagation function and learning rule determine the neural network's output. Equation (1) expresses the propagation function, which controls the inputs to the *jet* neuron from the outputs of the previous neurons.

$$P_t(t) = \sum_i 0_i(t) \times w_{ij} + b \dots \dots (1)$$

where the previous neuron's output is represented by Oi(t), the propagation function is represented by Pj (t), the weight is represented by wij, and the bias is represented by b.

It is possible to train a NN to do well with a certain set of inputs by adjusting its parameters according to a learning rule. As it learns, the network's weights are adjusted to improve output computation according to the learning rule[12].

Result Analysis and Discussion

Here we present the experimental outcomes of ML models trained on the Kaggle dataset using the Python simulation tool with the purpose of detecting financial fraud. For the purpose of assessing ML models' efficacy using a confusion matrix, recall,

accuracy, and precision. A dataset, performance metrics, ANN model output, and comparative analysis are detailed in the parts that follow.

Dataset Description

The dataset is extremely skewed since it includes fraudulent transactions (492 out of 284,807) from European cardholders in September 2013. PCA was used to convert the majority of the features in order to preserve privacy and secrecy. This produced 28 PCA-transformed numeric values (V1 through V28). The "Time" and "Amount" characteristics are the only ones that have not changed. This dataset is great for studies on financial fraud detection since the goal variable "Class" displays whether a transaction is fraudulent (1) or regular (0). The figure 2 shows the bar plot of (a) shows the total number of counts of each class and (b) shows the after SMOTE balanced approx. count plot.

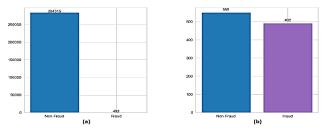


Figure 2: Count plot of after data balancing and before.

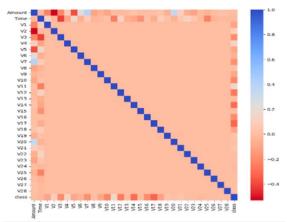


Figure 3: Correlation matrix of credit card dataset.

The associations between the many characteristics seen in Figure 3, such as "Time," "Amount," and anonymized variables "V1" to "V28," are represented visually by the credit card dataset's correlation matrix. The correlation coefficient among two variables is shown in each matrix cell, with colour intensity denoting the association's strength and direction. Shades of blue indicate significant negative connections, white or lighter colours show little to no link, and red hues indicate strong positive correlations. The diagonal line from the top left to the bottom right is solid red, indicating perfect positive correlation as each variable is compared with itself. This matrix is crucial for identifying patterns, relationships, and potential anomalies in the dataset, aiding in effective data analysis and decision-making.

Performance Measures

Four separate criteria were utilized to evaluate each model's performance: F1-score, recall, accuracy, and precision. These evaluation parameters are detailed below:

Citation: Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

1. Confusion Matrix

Confusion matrices, sometimes known as error matrices, may be used to display the performance of algorithms. The structure is a table. The matrix's rows show actual instances of the classes, while its columns show anticipated instances, or vice versa. It is used to calculate F1 scores, recall, precision, and accuracy [13]. The confusion matrix makes use of the following terms:

- **True Positive (TP):** This situation occurs when the expected and actual classes of a data point are both 1.
- **True Negative (TN):** A data point is considered to have this property when its anticipated and actual classes are both 0.
- **False Positive (FP):** This happens when a data point has a predicted class of 1 but a real class of 0.
- False Negative (FN): To put it simply, this happens when a data point has a real class of 1 but an anticipated class of 0.

2. Accuracy

A number of optimistic forecasts that are really right is measured by accuracy. As seen in equation (2), genuine positive / total projected positive is the ratio that determines precision in imbalanced classification:

$$Acuracy = \frac{TP + TN}{TP + TN + FN + FP} \dots (2)$$

3. Precision

Precision measures the effectiveness of a classifier in predicting positive samples. Simply divide the sum of all positive predictions by the number of actual positive samples, as shown in Equation (3), and you have the answer:

$$Precision = \frac{TP}{TP + FP} \dots (3)$$

4. Recall

The test result will accurately identify fraudulent transactions if recall is high. Recall, often called sensitivity, is defined as a ratio of TP to total real positives, as seen in equation (4):

$$Recall = \frac{TP}{TP + FN} \dots (4)$$

According to these measures evaluate a performance of ML models for financial fraud detection.

Experiment Results

An experimental outcome of several ML and DL models applied to the Credit Card Transaction dataset are displays in this section. An outcome is displayed using figures, graphs, and tables, providing a detailed overview of each model's performance.

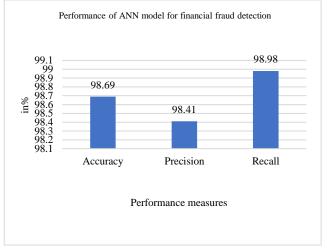


Figure 4: Financial Fraud Detection performance with ANN

The figure 4 shows the financial fraud detection performance with ANN model according to accuracy of 98.69%, precision of 98.41% and recall of 98.98%, respectively.

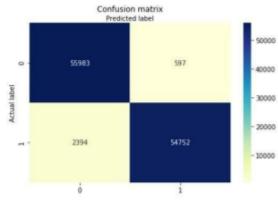


Figure 5: Confusion matrix for ANN Model.

Figure 5 shows the ANN model's confusion matrix, which clearly shows how well the model performed in detecting fraud. There were 55,752 cases of fraud (TP) and 55,983 cases of non-fraud (TN) that the model accurately recognised. However, it also made 597 FP errors, where non-fraudulent transactions were incorrectly flagged as fraud, and 2,394 false negative errors, where fraudulent transactions were missed. This matrix is crucial for evaluating the model's accuracy and reliability, highlighting areas where it performs well and where improvements are needed.

Comparative analysis

The table 2 below provides a comparative analysis of multiple DL and ML models used for financial fraud detection, specifically applied to a Credit Card Transaction dataset. For a thorough evaluation of the models' efficacy in identifying fraudulent behaviour in this domain, it details their performance indicators.

Citation: Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

Models	Accuracy	Precision	Recall
Decision Tree [14]	88	95	81
SVM [15]	72.3	60	96.4
ANN	98.69	98.41	98.98

Table 2: Comparison between various model for enhancing the performance of Financial Fraud Detection.

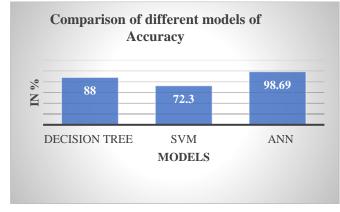


Figure 6: Comparison of different models of Accuracy

Figure 6 is a bar graph that shows how various models' accuracy is compared. The graph indicates that the ANN achieves the highest accuracy with a score of 98.69%, while the SVM model exhibits the lowest accuracy, scoring 72.3%.

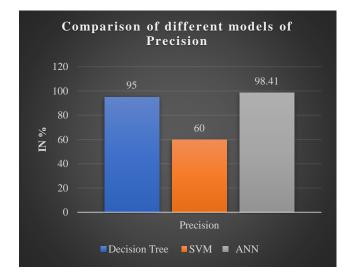


Figure 7: Comparison of different models of Precision.

Figure 7 illustrates the precision comparison among the models. The bar graph shows that the SVM model has the lowest precision score at 60%, while the ANN attains a highest precision with a value of 98.41%, respectively.

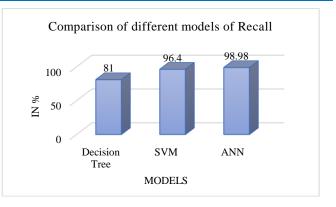


Figure 8: Comparison of different models of Recall.

The three models' recall scores are compared in Figure 8. The model that performs best in terms of memory is the ANN, which stands out with the greatest recall score of 98.98%. The DT model, on the other hand, has the lowest recall, at 81%.

This study's results show that when compared to more conventional ML models like DT and SVM, the ANN model performs far better in detecting financial fraud. The confusion matrix shows that the ANN achieves an outstanding accuracy98.69%, precision98.41%, and recall98.98% when it comes to properly recognising both fraudulent and nonfraudulent transactions. The comparative analysis highlights the ANN's significant advantages over the SVM, which exhibited the lowest accuracy (72.3%) and precision (60%), and the Decision Tree model, which, despite better precision (95%), lagged in recall (81%). These findings indicate that the ANN not only minimizes false positives and negatives effectively but also ensures a balanced performance across key metrics, suggesting that deep learning approaches are more adept at handling imbalanced datasets, making them particularly suitable for financial fraud detection applications.

Conclusion and Future Work

Frauds are said to be dynamic and lacking in patterns, making them difficult to identify. Fraudsters profit from new technological developments. They manage to circumvent all security measures, which leads to a massive financial loss. One way to keep tabs on fraudulent transactions is to use data mining techniques to analyze and detect unusual behaviors. Credit card transaction analysis has been the primary focus of this study's investigation into ML methods for financial fraud detection. ML's efficacy in differentiating between genuine and fraudulent transactions was proved via the application of classification models such as DT, SVM, and ANN. The most resilient model for fraud detection was ANN, which had the greatest performance among the models with accuracy (98.69), precision (98.41), and recall (98.98). The findings point to the value of ML for detecting financial crime and provide a way forward for creating better fraud prevention systems.

Future research can focus on incorporating more sophisticated DL models, like CNN or RNN, to further improve fraud detection performance. Additionally, hybrid models that combine various machine learning techniques may provide better accuracy in identifying fraudulent transactions. Another important aspect for future investigation is the application of real-time detection systems for fraud prevention, as well as

exploring methods for reducing false positives, which are critical in practical implementations. Model generalizability may be further improved by using more and more varied datasets.

References

- A. Mousa, "Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015," *J. Data Sci.*, vol. 14, no. 3, pp. 553–570, 2016, doi: 10.6339/jds.201607_14(3).0010.
- N. F. Ryman-Tubb, P. Krause, and W. Garn, "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Engineering Applications of Artificial Intelligence*. 2018. doi: 10.1016/j.engappai.2018.07.008.
- M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.
- S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, "Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement," *Technol. Manag. Rev.*, vol. 3, no. 1, pp. 46–62, 2018.
- H. Zhou *et al.*, "A distributed approach of big data mining for financial fraud detection in a supply chain," *Comput. Mater. Contin.*, 2020, doi: 10.32604/CMC.2020.09834.
- A. K. Rai and R. K. Dwivedi, "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme," in *Proceedings of the International Conference* on Electronics and Sustainable Communication Systems, *ICESC* 2020, 2020. doi: 10.1109/ICESC48915.2020.9155615.
- 7. S. Hidayattullah, I. Surjandari, and E. Laoh, "Financial statement fraud detection in indonesia listed companies using machine learning based on meta-heuristic optimization," in 2020 International Workshop on Big Data

and Information Security, IWBIS 2020, 2020. doi: 10.1109/IWBIS50925.2020.9255563.

- A. M. Mubalaike and E. Adali, "Deep Learning Approach for Intelligent Financial Fraud Detection System," in UBMK 2018 - 3rd International Conference on Computer Science and Engineering, 2018. doi: 10.1109/UBMK.2018.8566574.
- C. Gardner, D. C.-T. Lo, J.-C. Chern, P. Paschos, and C. Ng, "Tiered Financial Fraud Detection Utilizing Precision Stratified Random Forest Assembly," in 2019 IEEE 5th International Conference on Big Data Intelligence and Computing (DATACOM), 2019, pp. 254–257. doi: 10.1109/DataCom.2019.00047.
- M. Erfani, F. Shoeleh, and A. A. Ghorbani, "Financial Fraud Detection using Deep Support Vector Data Description," in *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, 2020. doi: 10.1109/BigData50022.2020.9378256.
- G. K. Arun and K. Venkatachalapathy, "Convolutional Long Short Term Memory Model for Credit Card Detection," in *Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA* 2020, 2020. doi: 10.1109/ICECA49313.2020.9297606.
- A. Khashman and K. Dimililer, "Neural networks arbitration for optimum DCT image compression," in EUROCON 2007 - The International Conference on Computer as a Tool, 2007. doi: 10.1109/EURCON.2007.4400236.
- H. M and S. M.N, "A Review on Evaluation Metrics for Data Classification Evaluations," *Int. J. Data Min. Knowl. Manag. Process*, 2015, doi: 10.5121/ijdkp.2015.5201.
- K. Kumain, "Analysis of Fraud Detection on Credit Cards using Data Mining Techniques," *Turkish J. Comput. Math. Educ.*, 2020, doi: 10.17762/turcomat.v11i1.13590.
- D. Zhang, B. Bhandari, and D. Black, "Credit Card Fraud Detection Using Weighted Support Vector Machine," *Appl. Math.*, vol. 11, no. 12, pp. 1275–1291, 2020, doi: 10.4236/am.2020.1112087.

Copyright: © 2023 Eswar Prasad G. This Open Access Article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.