



<https://doi.org/10.15407/economyukr.2026.07.027>

JEL: C45, C55, C88, G20, G29

BENKHELOUF Rachid, Dr. Sci. (Econ.), Department of Economic Sciences

University Centre of Maghnia

Al-Zawiya Road, 13300, Maghnia, Algeria

e-mail: r.benkhelouf@cu-maghnia.dz

ORCID: <https://orcid.org/0000-0001-9535-7237>

BEKADDOUR Fatima Zohra, Dr. Sci. (Econ.), Department of Economic Sciences

University of Ghardaia

Ghardaia, PO Box 455b, 47000, Algeria

e-mail: bekaddour.fatimazohra@univ-ghardaia.edu.dz

ORCID: <https://orcid.org/0000-0002-1864-8716>

A COMPARATIVE ANALYSIS OF ARTIFICIAL NEURAL NETWORKS AND RANDOM FORESTS FOR FINANCIAL TRANSACTION FRAUD DETECTION

Fraud detection in financial transactions is a critical challenge due to rising fraudulent activities. This study compares Artificial Neural Networks (ANN) and Random Forest models using 10,000 transaction records. Performance was evaluated with accuracy, recall, and F1-score, showing ANN at 90.2% and Random Forest at 96.5%. Key features influencing fraud detection included transaction time, day, amount, identifier, and merchant. Findings highlight the effectiveness of supervised machine learning in improving fraud detection efficiency.

Keywords: Random Forest; Artificial Neural Network; fraud detection; machine learning algorithms.

Fraudulent transactions pose a significant challenge to the financial sector, threatening both the economic stability of institutions and the trust of individual consumers. The rapid advancement of technology, particularly in artificial intelligence (AI) and machine learning has opened new avenues for detecting fraudulent activities effectively.

Citation: Benkhelouf, R., Bekaddour, F.Z. (2026). A comparative analysis of Artificial Neural Networks and Random Forests for financial transaction fraud detection. *Economy of Ukraine*. 69. 07(776). 27—43. <https://doi.org/10.15407/economyukr.2026.07.027>

© Publisher PH «Akademperiodyka» of the NAS of Ukraine, 2026. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

Detecting fraud in real-time is critical for maintaining the integrity of financial systems, especially in online banking and *e-commerce* platforms. AI algorithms, such as the K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), and various regression-based methods, have emerged as robust tools that can improve the precision and recall of fraud detection efforts, helping organizations quickly respond to potential threats (Chung, Lee, 2023). As financial transactions become increasingly digital, the datasets used for training fraud detection models also undergo significant changes, often leading to imbalanced datasets characterized by a minor proportion of fraudulent activities compared to legitimate transactions. This imbalance can adversely affect the model's predictive performance, demanding innovative solutions to create effective detection systems (Awosika et al., 2024). Recent developments have highlighted the potential of Federated Learning (FL) alongside Explainable AI (XAI) to overcome challenges related to data privacy and transparency while ensuring high-performance metrics.

FL allows multiple financial institutions to collaboratively build a fraud detection model without the direct sharing of sensitive customer data, thus adhering to stringent privacy regulations. The integration of XAI further enhances the system by providing human interpretable insights, helping experts validate and trust model predictions. Overall, the emergence of these advanced technologies represents a transformative shift in the field of financial fraud detection, indicating a promising future where safety and privacy can effectively coexist.

Modern technologies, particularly artificial intelligence (AI) and the Internet of Things (IoT), are key drivers reshaping many scientific and industrial fields. In recent years, we have witnessed a significant increase in the use of these technologies to improve efficiency, foster innovation, and provide effective solutions to complex challenges facing society (Yao et al., 2019). The studies compiled in this paper address a variety of applications, reflecting the wide variety of uses of AI (Sorkun, Toraman, 2017).

Furthermore, some research focuses on the applications of artificial intelligence in human resource management, analyzing the impact of these technologies on improving administrative processes and increasing decision-making effectiveness (Hamal, Senvar, 2021). The use of machine learning models in detecting financial fraud is also being explored, reflecting the importance of these technologies in enhancing transparency and accountability in financial systems (Albizri et al., 2019).

These documents highlight the importance of research and development in the field of artificial intelligence and the Internet of Things and emphasize the need for collaboration between academia and industry to develop innovative solutions that meet societal needs and contribute to achieving sustainable development. These studies are not merely academic research; they represent practical steps toward achieving a smarter and more sustainable future.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR FRAUDULENT TRANSACTION DETECTION: A CONCISE REVIEW

Financial institutions face many risks associated with fraudulent transactions. The impact of fraudulent transactions is substantial, affecting not just the financial institution's assets, but also the customer's trust in that institution. Although there are far more legitimate than fraudulent transactions, the number of fraudulent transactions is still significant enough that there exists a highly disproportionate number of each category in the datasets used to develop fraud-detection models. This scarcity of fraud in training sets degrades the model's ability to discriminate between legitimate and fraudulent transactions, often generating model outputs of high false negative and false positive rates. These rates of error, depending on the type of error, will compromise both the security and user experience of the model (Awosika et al., 2024). To address these issues, many institutions have begun to implement advanced AI or algorithmic systems, the most used of which are Federated Learning (FL) and Explainable AI (XAI). FL provides a method for different institutions to train fraud-detection models together without violating the data-sharing restrictions of privacy laws or sharing civilly protected sensitive customer records. XAI will improve the transparency of how the algorithmic system is making a fraud-detection decision and allow a human subject matter expert to better understand any given algorithmic decision that was made thereby enhancing their level of trust in the algorithmic result and decision.

Credit card fraud, identity theft, account takeover, and money laundering are all examples of common forms of fraud. Credit card fraud usually happens when someone uses card information without permission, especially when the card isn't present, such as when you buy something online. Identity theft is when crooks steal personal information to take on someone else's identity and create accounts or make fake purchases. Account takeover employs phishing attacks or data breaches to get into user accounts, while money laundering uses long chains of transactions to hide where illegal money came from (Ashfaq et al., 2022). Each sort of fraud creates unique patterns in transaction data, which makes them good candidates for machine learning research. But fraud techniques are always changing, so detection systems need to keep up with new trends.

Fraud hurts businesses in both their reputation and their finances. Unauthorized transactions can cost businesses money directly, and they can also cost them money indirectly by making them spend more on fraud investigation and prevention. Also, continuous fraud can make customers lose faith and lead to legal problems. Different types of fraud affect different types of businesses. For example, shops deal with credit card fraud more regularly, whereas banks deal with more advanced types of fraud, including identity theft and money laundering (West et al., 2015). This heterogeneity demands personalized detection tactics and shows how important it is to have AI frameworks that can be changed to fit the risks and changing patterns of fraud in each area.

AI stands for technology that mimics human cognitive processes, including learning, thinking, and making decisions. In finance, AI uses machine learning and deep learning algorithms to look at transaction data and tell the difference between real and fake behavior (Nguyen et al., 2020). A major problem is class imbalance, which means that there are a lot more real transactions than fake ones (Awosika et al., 2024). To deal with this, sophisticated models like autoencoders, long-short-term memory (LSTM) networks and convolutional neural networks (CNNs) are employed to find small problems. Combining behavior-based techniques with genetic algorithms in hybrid models can lower the number of false positives while keeping the number of true positives high. XAI makes things even more clear, and Federated Learning (FL) lets schools exchange model learning without giving out private information, which is a good way to keep privacy.

Machine learning approaches differ from classical approaches due to their ability to be flexible and adaptable whereas classical statistical and rule-based models have been used (e.g., logistic regression, decision trees, and naive Bayes) and provide good interpretive ability but do not capture the dynamic nature of fraud effectively, especially in highly skewed datasets (Ishangediok, Gajamannage, 2022). In addition, they typically have low precision and require significant time for training. Furthermore, machine learning approaches can evolve with new data and have the potential to identify anomalies in large transactional data. Advanced techniques such as Support Vector Machines (SVM) or Hidden Markov Models (HMM) may offer better means of identifying transactions that are unusual compared to classical models. Additionally, the use of ensemble methods such as Random Forests and boosting and hybrid designs that blend traditional statistics with neural networks will further improve the performance of machine learning methods by decreasing the frequency of classification errors (Nguyen et al., 2020). Additionally, deep learning methodologies (such as autoencoders, CNNs, and LSTMs) have shown clearly superior results compared with rule-based systems.

AI-based systems that detect fraud use numerous methods to identify fraudulent transactions through credit cards. An example includes multiple methods of classification, including decision trees, Artificial Neural Networks (ANN), LSTM and CNN will classify a credit-card transactions as either legitimate or fraudulent (Nguyen et al., 2020). Most of the models have Predictive Analytics Technologies (PAT) as their supports, which can be used to find anomalies (e.g., unusual installations for purchase, number of consecutive transactions or behavior outside the historical norm of a user). Hidden Markov Models (HMM) compute log transaction and risk profiles while using behavior-based algorithms to cluster transactions for the purpose of identifying transactions that deviate from normal behavior. Genetic algorithms assist in determining optimal thresholds for identifying suspicious activity for improved precision and recall. Recent research by J. Chung & K. Lee (2023) proposes a combination of K-Nearest Neighbors (KNN) techniques, Linear Discriminant Analysis (LDA) and regression techniques, to realize higher levels of recall in real time applications involving online banking.

Supervised learning techniques use labeled datasets to tell if each transaction is authentic or false. Some common supervised methods include Logistic Regression (LR), KNN, SVM, Decision Trees (DT), Random Forest (RF), and Extreme Gradient Boosting (XGB). For instance, X. Niu et al. (2019) use a public credit card dataset of 284,807 transactions (492 of which were fraudulent) to train these models. They find that XGB and RF acquire AUROC scores of 0.989 and 0.988, respectively. This means that they are better at discovering fraud than other methods that don't use supervision. Researchers are investigating ensemble and hybrid designs, such as the integration of KNN with LDA or decision trees with Random Forests, to further enhance accuracy and recall (Chung, Lee, 2023). You need to carefully build the characteristics of these models and change their settings so that they can deal with new forms of fraud.

Unsupervised learning is quite helpful for finding fraud when there isn't a lot of labeled data. Techniques like One-Class SVM, Autoencoders, Restricted Boltzmann Machines (RBM), and Generative Adversarial Networks (GAN) learn the normal distribution of transactions and mark big differences as possible fraud (Niu et al., 2019). One-Class SVM establishes a limit for normal data, categorizing points outside this boundary as anomalies. In contrast, autoencoders compress inputs into a latent space and subsequently rebuild them, identifying fraud through significant reconstruction errors. Hybrid systems that use both unsupervised anomaly detection and supervised classifiers take advantage of the best parts of both types of systems, making detection stronger when transaction patterns change (Chung, Lee, 2023).

Neural networks are very effective at identifying large transaction datasets' complex, nonlinear characteristics. The multiple levels found in deep architectures allow these systems to incrementally identify features (from simple transaction characteristics through to more abstract behavioral characteristics such as time, location, and order of spending), with higher levels of feature extraction providing improved accuracy and recall, enabling real-time monitoring and timely response to suspicious transactions. To reduce the risk of overfitting and enhance the ability of the network to generalize to previously unseen data banks, it can create timely fraud alerts, lower potential losses, and improve customer confidence in digital payment systems through the use of techniques such as dropout and batch normalization.

For identifying fraudulent transactions, anomaly detection methods have a center role, commonly described under unsupervised learning, since they allow for the automated analysis of large amounts of information with little to no labeled (shared) information (DeLise, 2023). One such example is Deep SAD, a deep-learning-based framework for detecting anomalies in very high-frequency trading environments, which has outperformed more traditional unsupervised methods. In the case of credit card monitoring, numerous algorithms, including Random Forest, Logistic Regression, Decision/Tree-based models, Support Vector Machine (SVM) and Neural Networks have been tested, however, they are challenged by the imbalanced characteristics of the data being analyzed and the user behaviors changing over time (Moschini et al., 2021). Recently, there have been attempts to exa-

mine the problem of classification using classification through anomaly detection and through the use of Time Series models like ARIMA and rolling windows. Hybrid methods that combine supervised and unsupervised learning, incorporating feedback systems to adjust the underlying model used to evaluate transaction outcomes will likely lead to more adaptive and accurate real-time methods of detecting fraud.

Numerous studies have explored financial misstatement detection and fraud identification using various machine learning and statistical techniques. E. Zavisanos et al. (2025) introduced a TabTransformer model with a gated multi-layer perceptron to improve financial misstatement detection, addressing class imbalance with a focal loss function. Similarly, S. Gupta & S. Mehta (2024) reviewed data mining classification techniques for financial fraud detection, emphasizing the importance of mapping fraudulent and non-fraudulent companies to improve classification accuracy. Y. Işık et al. (2023) tested artificial neural networks and decision tree methods, achieving over 99% accuracy in fraud detection. L. Hernandez Aros et al. (2024) reviewed financial fraud detection using machine learning, addressing its negative impact on organizational administration and profit maximization for owners/investors. Applying PRISMA and Kitchenham methods, they examined 104 articles (2012—2023) from Scopus, IEEE Xplore, Taylor & Francis, SAGE, and Science Direct, selected via predefined criteria. The review analyzed articles, authors, sources, countries, trends, and datasets to identify financial fraud types. Machine learning models and metrics assessed performance, revealing a trend toward real datasets. Credit card fraud detection models were the most prevalent, often using data from stock exchanges in China, Canada, the US, Taiwan, and Tehran. Synthetic data usage remained low (under 7%).

Other studies focused on advanced fraud detection mechanisms. H. Shilpa (2023) highlighted data mining techniques for financial fraud identification, particularly in fiscal summary deceptions. İ. Kılıç & S. Önal (2022) developed an artificial neural network model to assess financial fraud risks, achieving an 88.89% accuracy rate. S. Hamal & Ö. Senvar (2021) evaluated machine learning classifiers in detecting financial fraud among Turkish SMEs, concluding that the random forest model with oversampling was the most effective. M. Riskiyadi (2024) compared machine learning models for financial fraud detection, finding that Extremely Randomized Trees (ERT) with an 80:10 training-testing split was the most accurate.

Several studies investigated biometric and AI-driven verification systems to enhance financial security. P. William et al. (2023) examined biometric verification methods, such as signature authentication, using neural networks. P. Tamrakar & A. Badholia (2022) reviewed the evolution of signature verification systems, emphasizing deep learning's role in improving accuracy.

Broader applications of AI and IoT in security and monitoring were also discussed. P. William et al. (2023) proposed an IoT-enabled surveillance robot for border security, while N. Darwante et al. (2023) designed a surveillance robot with remote control capabilities for combat zones. In a related study, P. Chavan et al. (2023) explored the impact of Extra High Voltage (EHV) transmission lines on human health and the environment.

Beyond fraud detection, AI applications in other domains were explored. G. Endait et al. (2023) utilized machine learning for automated leaf disease detection in precision agriculture. P. William et al. (2023) investigated AI-driven customer service chatbots, while G. Sasipriya & B. Lavanya (2023) applied natural language processing (NLP) techniques to extract information from nanomaterial science research.

TARGET SETTINGS

Machine learning, artificial intelligence, and data mining are becoming increasingly valuable tools for detecting financial fraud, enhancing security, and optimizing technology use. Several previously published studies have explored the use of machine learning and statistical methods to identify financial misstatements and financial fraud (e.g., Zavitsanos et al. 2025; Gupta, Mehta 2024; Işık et al. 2023; Hernandez Aros et al. 2024); however, there has been little research comparing models or methodology for handling imbalanced data sets. Previous research on the use of ANNs and decision trees has provided advanced modeling with high accuracy; however, there is a dearth of comparative studies available.

The **purpose of this study** is to eliminate these gaps in the literature by providing a systematic comparison of artificial neural networks and random forest models (in real-world financial fraud data) in order to provide empirical evidence of their comparative strengths as well as generate utility derived from the analysis of these two methods for financial institutions.

Methodology and data. The research team is working to create fraud detection systems that leverage machine learning and deep learning algorithms to classify online transactions as genuine or fraudulent based on transaction databases. However, identifying fraudulent online transactions is becoming increasingly chal-

Table 1. Functions in the transaction data set

Transactions Feature Name	Description
Transaction ID	Unique identifier for each transaction
Amount	The monetary value of the transaction
Type	Type of transaction, either "Credit" or "Debit"
Merchant	The merchant involved in the transaction, such as Amazon, Walmart, or Target
Location	Location of the transaction, categorized as "Local" or "International"
Time	The hour of the day when the transaction occurred
Day of Week	The day of the week when the transaction occurred
Account Type	Type of account associated with the transaction, either "Personal" or "Business"
Fraudulent	Binary indicator denoting whether the transaction is fraudulent (1) or not (0)

Source: compiled by the authors from: *Kaggle*. URL: <https://www.kaggle.com/datasets/userabc12541874/audit-data> (accessed: 04.03.2025).

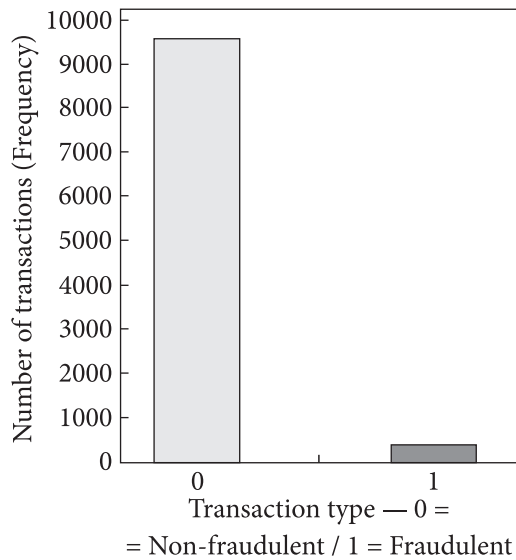


Fig. 1. Distribution of transaction. Distribution of “Fraudulent” with columns split by “Fraudulent”

Source: by the authors using Orange software.

lending as illicit payment patterns evolve to closely mimic legitimate transaction characteristics.

We collected the dataset called AUDIT_DATA from Kaggle Depository for fraud transaction detection. The dataset consists of 10 000 records with 08 features.

Audit Description. The audit was conducted on a company named

“E-Commerce” a large online retail platform known for its diverse range of products and global presence. The audit aimed to assess the integrity of financial transactions processed through the company’s platform over a specified period.

Data Collection. Transaction data was collected from the company’s database, including information such as transaction IDs, amounts, transaction types, merchant details, transaction locations, timestamps, account types, and fraud indicators. The features of the fraudulent transaction dataset are shown in Table 1.

This dataset structure is well-designed for fraud detection modeling, containing key transaction attributes that capture both financial aspects (Amount, Type, Account Type) and contextual information (Merchant, Location, Time, Day of Week). The inclusion of temporal features (Time and Day of Week) is particularly valuable, the binary target variable “Fraudulent” makes this suitable binary classification models like the Random Forest and Neural Network implementations.

The dataset shown in Fig. 1 reveals a significant skewed class balance, with fraudulent transactions making up just 4.69% of all cases, or 469 transactions, while non-fraudulent transactions accounted for 9,531.

This skewed distribution poses a critical challenge for machine learning model development. When training data is this unbalanced, the model becomes disproportionately influenced by the majority class (non-fraudulent transactions), which can compromise its ability to accurately detect fraud cases.

This imbalance creates a risk that the model will be biased toward identifying transactions as legitimate, potentially missing actual fraud cases, since it has been predominantly exposed to non-fraudulent examples during training.

THE USE OF ALGORITHM IN ORANGE SOFTWARE

The ANN algorithm was utilized in the Orange software to achieve high-accuracy solutions and to improve the model through a scientific approach inspired by neural cells in biological sciences. This approach studies genes to detect diseases, explore mutations, and investigate other genetic phenomena.

On the other hand, the random forests are not biologically inspired instead, they are rooted in statistics and probability theory, and they are an extension of the decision tree method.

MODELING

Mechanism for applying the Artificial Neural Network Algorithm. After processing the data and imputing missing values, the variables were encoded as a fundamental step. The data was then split into 80% training data and 20% testing data.

The Artificial Neural Network was designed and trained to classify financial transactions as a set of independent variables. The Adam Solver function was used, demonstrating good performance. Additionally, the ReLU activation function was adopted, as it outperformed the Tanh and Logistic functions in classifying the types of fraud in financial data. The number of neurons in the hidden layers was set to 50 neurons to train the ANN.

The accuracy of the ANN model reached 90%, while the area under the ROC curve (AUC) was 0.808.

The configuration parameters for a Random Forest model:

Number of trees — 10 (relatively small for a Random Forest, which typically benefits from more trees),

Maximal number of considered features — unlimited (the model can consider all available features for splitting decisions),

Replicable training — No (results won't be exactly reproducible across runs),

Maximal tree depth — unlimited (trees can grow without depth restrictions),

Stop splitting nodes with maximum instances — 5 (nodes won't be split further if they contain 5 or fewer instances).

This configuration represents a fairly basic Random Forest implementation with minimal restrictions on tree growth. The small number of trees (10) might limit the model's performance compared to a larger ensemble, though this depends on the specific dataset characteristics. The unlimited depth and feature consideration could potentially lead to overfitting, but the minimum node size of 5 provides some regularization.

RESULTS AND DISCUSSION

Performance metrics. The key performance metrics (AUC, Accuracy, Precision, Recall, F1) for each model are presented (Table 2).

The accuracy of the Random Forest (RF) model reached 96%, while the area under the ROC curve (AUC) was 0.997.

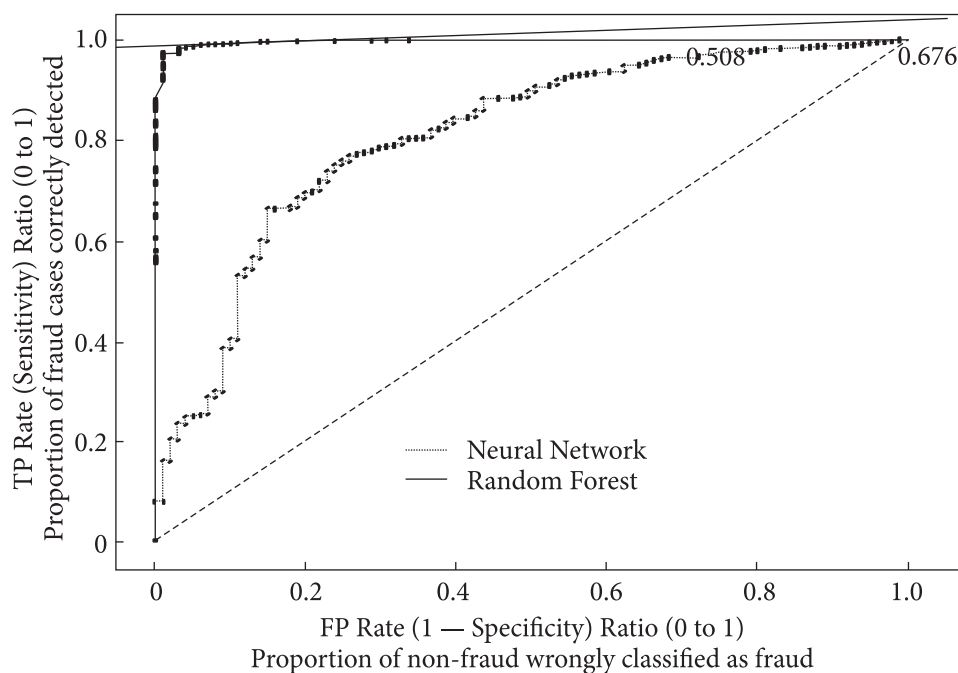


Fig. 2. Roc Analysis on April 5, 2025. Target class: 0; Costs: FP = 500, FN = 500; Target probability: 95%

Source: by the authors using Orange software.

Table 2. Performance metrics

Model	AUC	CA	F1	Prec	Recall
Artificial Neural Network	0.808	0.950	0.925	0.902	0.950
Random Forest	0.997	0.964	0.954	0.965	0.964

Source: by the authors using Orange software.

The Random Forest model clearly outperforms in most metrics, especially in AUC and Precision, making it the overall best. The Artificial Neural Network provides strong and stable performance but is less efficient compared to the Random Forest.

Roc curve. The ROC curve is a graphical representation of a binary classifier model's performance, created by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR) at different classification thresholds. TPR is the proportion of positive cases correctly classified, while FPR is the proportion of negative cases incorrectly classified as positive.

From the Fig. 2, it is evident that there is a 0.676 probability of errors or discrepancies in the financial data and the probability of the random forest of the type 0 it is 0.508. Additionally, the probability of a Type 1 error in classifying fraud is 0.324, which indicates the reliability and accuracy of the financial data, as they are free from significant errors or discrepancies. As previously mentioned, this curve serves as a useful metric for evaluating the performance of binary classification models.

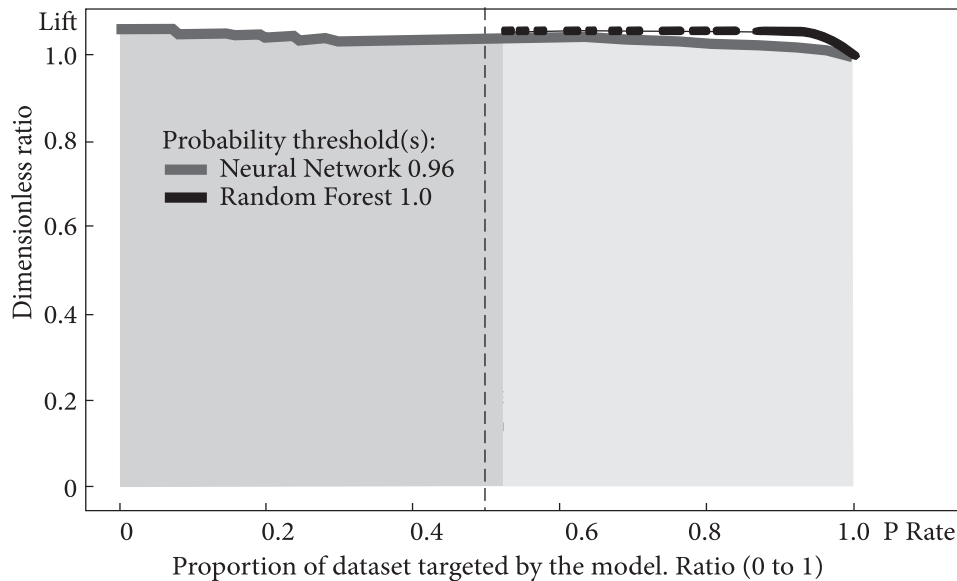


Fig. 3. Performance Curve on April 5, 2025. Target class = 0
Source: by the authors using Orange software.

The Fig. 2 also shows that the Random Forest algorithm exhibits ideal performance due to the ROC curve aligning closely with the upper-left corner and covering a larger area under the curve (AUC), reflecting the quality of this test. This highlights the model's effectiveness in accurately interpreting and classifying fraud by type, as evidenced by the curve's value.

The Area under the Receiver Operating Characteristic Curve (AUC-ROC) is a metric used to measure the classifier's ability to distinguish between positive and negative classes.

HOSMER & LEMESHOW suggest that the values of the area under the ROC curve (AUC-ROC) can be interpreted as follows:

ROC = 0.5: The model has no discriminatory power, equivalent to random chance,

$0.7 \leq \text{ROC} \leq 0.8$: The model has acceptable discriminatory power,

$0.8 \leq \text{ROC} \leq 0.9$: The model has excellent discriminatory power,

$\text{ROC} \geq 0.9$: The model has outstanding discriminatory power.

Performance Curve. To further evaluate the model and validate its results, as well as to assess its ability to detect and identify fraud with high accuracy, it is recommended to use the performance curve for the neural network algorithm. This curve illustrates the relationship between the true positive rate (sensitivity) and the false positive rate (specificity) at different probability thresholds. The curve helps in identifying the optimal probability threshold that balances the trade-off between the true positive rate and the false positive rate (Fig. 3).

Calibration plot. We observe a probability threshold of 1, meaning excellent performance in classifying fraudulent transactions using the Random Forest model compared to the Artificial Neural Network model (Fig. 4).

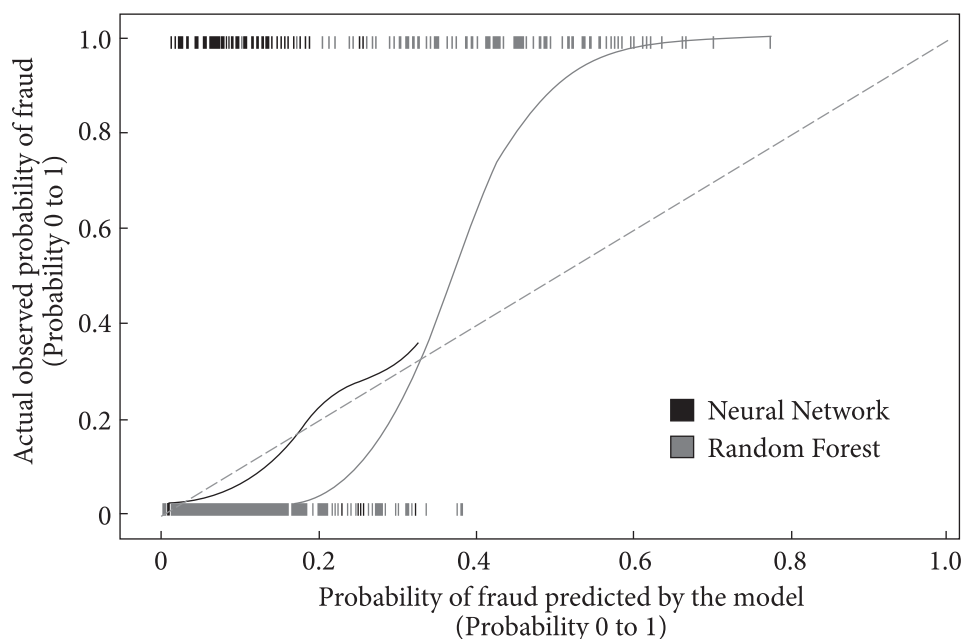


Fig. 4. Calibration plot on April 5, 2025. Target class: 1, Output model calibration: Sigmoid calibration

Source: by the authors using Orange software.

This is a calibration plot comparing Neural Network and Random Forest models for fraud detection. The plot shows:

- Target class is 1 (fraudulent transactions) with sigmoid calibration applied,
- The x-axis represents predicted probability while the y-axis shows calibration curve values,
- The Random Forest model shows better calibration characteristics than the Neural Network model, particularly in the middle probability range (0.3—0.6),
- The Random Forest curve approaches the ideal diagonal line more closely at higher probability thresholds (0.6+),
- The Neural Network model appears to overestimate probabilities in the lower range (0.2—0.4) as shown by its curve being above the diagonal,
- Both models' predictions converge at very high probabilities (0.8+).

This suggests the Random Forest model offers more reliable probability estimates for fraud detection, which is crucial for setting appropriate decision thresholds in production systems.

The confusion matrix. The confusion matrix cells represent the Random Forest model predictions, providing a summary of the model's predictive ability to classify error types, as shown in the Fig. 5. Each row indicates the actual true class and each column indicates the predicted class.

The matrix (Table 3) shows the following classifications:

True Positive (TP): 28 values were correctly predicted by the model, where the model forecasted the presence of fraud in 28 cases, which actually contained fraud,

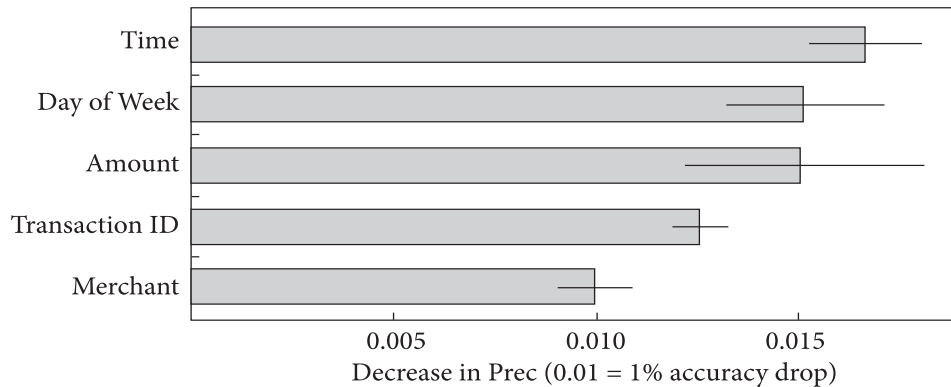


Fig. 5. Feature Importance on April 5, 2025. Score: Prec; Permutations: 5
Source: by the authors using Orange software.

Table 3. Confusion Matrix for Random Forest (Number of Instances)

	Predicted			
		0	1	Σ
Actual	0	1899	0	1899
	1	73	28	101
	Σ	1972	28	2000

Source: by the authors using Orange software.

True Negative (TN): The model correctly predicted that 1899 cases were free of fraud, compared to 1899 actual cases that did not contain fraud,

False Positive (FP): The model did not incorrectly predict any case as being free of fraud while it actually contained fraud, with a value of 0, indicating no instances of false predictions in this context,

False Negative (FN): 73 values were incorrectly predicted by the model, where it forecasted that they were free of fraud while they actually contained fraud, reflecting the presence of undetected fraud cases.

The confusion matrix shows us the accuracy of results based on model performance. The figure represents values and their probabilities where actual values intersect with predicted percentages from the Random Forest model.

Feature Importance.

This Fig. 5 shows a Feature Importance plot for the Random Forest using Precision (Prec) as the scoring metric with 5 permutations:

- Time is the most important feature, with approximately 0.016 decrease in precision when permuted,
- Amount and Day of Week are tied for second most important (around 0.015 decrease in precision),
- Transaction ID ranks fourth (about 0.012 decrease),
- Merchant has the least impact (approximately 0.010 decrease).

This suggests that Time and Amount are particularly important for reducing false positives in fraud detection.

FUTURE RESEARCH DIRECTIONS

After presenting the results reached, they must be discussed by giving them their place in their field and comparing them with previous studies, showing their extent and opposition to previous results

Future studies could expand by using larger and more diverse datasets drawn from different sectors, such as banking institutions, payment platforms, and *e-commerce* systems, to assess the generalizability of the results. Current machine learning models could also be compared with additional algorithms, including advanced deep learning models, to evaluate their effectiveness in improving the accuracy of fraud detection.

Moreover, incorporating additional explanatory variables related to customer behavior and transaction patterns could further enhance the predictive capability of fraud detection systems. Future research could also explore the integration of artificial intelligence techniques with auditing and internal control procedures, supporting auditors and financial institutions in managing fraud risks and improving the efficiency of transaction monitoring systems.

CONCLUSION

Based on the performance metrics of precision, recall, and F1 score, it is evident that the Random Forest model outperforms the Neural Network model, particularly in terms of precision and the area under the curve (AUC). This indicates a high balance in predictions for both positive and negative cases.

The feature importance analysis suggests that time and day of the week, followed by the amount and transaction ID, play a significant role in detecting fraudulent transactions, as they are among the most important features in improving the model's performance.

This study has demonstrated the effectiveness of machine learning algorithms in fraud detection, with the Random Forest model outperforming the Artificial Neural Network model. The Random Forest achieved 96% accuracy and an exceptional AUC of 0.997, indicating outstanding discriminatory power according to Hosmer & Lemeshow's guidelines. Time and transaction amount emerged as the most critical features for fraud detection. Despite the challenge of class imbalance (only 4.69% fraudulent transactions), the models successfully classified transactions with high precision. The results suggest that Random Forest models provide more reliable probability estimates for fraud detection systems, making them particularly valuable for financial security implementations.

The study recommends that financial institutions and *e-commerce* companies leverage machine learning algorithms by integrating them into their operational systems to detect fraudulent transactions. This integration helps internal auditors identify high-risk transactions and make timely decisions regarding them.

The study also suggests that variables reflecting the temporal characteristics of financial operations have a stronger impact on effectively detecting and identifying patterns of fraudulent transactions.

Funding. The article was prepared on our own initiative, on a free basis.

Conflict of interest. There are no financial or personal conflicts of interest that could have influenced the writing of this article.

Involvement of AI. Artificial intelligence tools were used only for language editing and proofreading. The scientific content, analysis, interpretation, and conclusions remain entirely the responsibility of the authors.

REFERENCES

- Chung, J., Lee, K. (2023). Credit Card Fraud Detection: An Improved Strategy for High Recall Using KNN, LDA, and Linear Regression. *Sensors*. 23(18). 7788. <https://doi.org/10.3390/s23187788>
- Awosika, T., Shukla, R., Pranggono, B. (2024). Transparency and privacy: The role of explainable ai and federated learning in financial fraud detection. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2024.3394528>
- Yao, J., Pan, Y., Yang, S., Chen, Y., Li, Y. (2019). Detecting fraudulent financial statements for the sustainable development of the socio-economy in China: A multi-analytic approach. *Sustainability*. 11(6). 1579. <https://doi.org/10.3390/su11061579>
- Sorkun, M., Toraman, T. (2017). Fraud detection on financial statements using data mining techniques. *Intelligent Systems and Applications in Engineering*. 5(3). 132—134. <https://doi.org/10.18201/ijisae.2017531428>
- Hamal, S., Senvar, Ö. (2021). Comparing performances and effectiveness of machine learning classifiers in detecting financial accounting fraud for Turkish SMEs. *Int. J. Comput. Intell. Syst.* 14(1). 769—782. <https://doi.org/10.2991/ijcis.d.210203.007>
- Albizri, A., Appelbaum, D., Rizzotto, N. (2019). Evaluation of financial statements fraud detection research: A multi-disciplinary analysis. *International Journal of Disclosure and Governance*. 16(4). 206—241. <https://doi.org/10.1057/s41310-019-00067-9>
- Ashfaq, T., Khalid, R., Yahaya, A., Aslam, S., Azar, A., Alsafari, S., Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*. 22(19). 7162. <https://doi.org/10.3390/s22197162>
- West, J., Bhattacharya, M., Islam, R. (2015). Intelligent Financial Fraud Detection Practices: An Investigation. In: J. Tian, J. Jing, Srivatsa, M. (Eds.). International Conference on Security and Privacy in Communication Networks. SecureComm 2014. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Vol. 153. Springer, Cham. https://doi.org/10.1007/978-3-319-23802-9_16
- Nguyen, T., Tahir, H., Abdelrazek, M., Babar, A. (2020). Deep learning methods for credit card fraud detection. *arXiv Preprint arXiv:2012.03754*. <https://doi.org/10.48550/arXiv.2012.03754>
- Isangediok, M., Gajamannage, K. (2022). Fraud detection using optimized machine learning tools under imbalance classes. *IEEE*. 4275—4284. <https://doi.org/10.1109/BigData55660.2022.10020723>
- Niu, X., Wang, L., Yang, X. (2019). A comparison study of credit card fraud detection: Supervised versus unsupervised. *arXiv Preprint arXiv:1904.10604*. <https://doi.org/10.48550/arXiv.1904.10604>
- DeLise, T. (2023). Deep semi-supervised anomaly detection for finding fraud in the futures market. *arXiv Preprint arXiv:2309.00088*. <https://doi.org/10.48550/arXiv.2309.00088>

- Moschini, G., Houssou, R., Bovay, J., Robert-Nicoud, S. (2021). Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model. *Engineering Proceedings*. 5(1). 56. <https://doi.org/10.3390/engproc2021005056>
- Zavitsanos, E., Kelesis, D., Paliouras, G. (2025). Calibrating TabTransformer for financial misstatement detection. *Applied Intelligence*. 55(1). 3. <https://doi.org/10.1007/s10489-024-05861-9>
- Gupta, S., Mehta, S. (2024). Data mining-based financial statement fraud detection: Systematic literature review and meta-analysis to estimate data sample mapping of fraudulent companies against non-fraudulent companies. *Global Business Review*. 25(5). 1290—1313. <https://doi.org/10.1177/0972150920984857>
- Işık, Y., Kefe, İ., Sağlar, J. (2023). Detection of fraudulent transactions using artificial neural networks and decision tree methods. *Business & Management Studies: An International Journal*. 11(2). 451—467. <https://doi.org/10.15295/bmij.v11i2.2200>
- Hernandez Aros, L., Bustamante Molano, L., Gutierrez-Portela, F., Moreno Hernandez, J., Rodriguez Barrero, M. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*. 11(1). 1130. <https://doi.org/10.1057/s41599-024-03606-0>
- Shilpa, H. (2023). Analyzing the Bank Scam's Financial Fraud and its Technological Repercussions using Data Mining. In: IEEE, 2023 Second International Conference on Electronics and Renewable Systems (ICEARS). P. 1553—1559. <https://doi.org/10.1109/ICEARS56392.2023.10085354>
- Kılıç, İ., Önal, S. (2022). Finansal hilelerin tespit edilmesinde kullanılan veri madenciliği yöntemleri ve borsa istanbul'da bir uygulama. *Muhasebe ve Denetime Bakış*. 22(67). 181—208. <https://doi.org/10.55322/mdbakis.1068503>
- Riskiyadi, M. (2024). Detecting future financial statement fraud using a machine learning model in Indonesia: A comparative study. *Asian Review of Accounting*. 32(3). 394—422. <https://doi.org/10.1108/ARA-02-2023-0062>
- William, P., Lanke, G., Bordoloi, D., Shrivastava, A., Srivastava, A., Deshmukh, S. (2023). Assessment of human activity recognition based on impact of feature extraction prediction accuracy. In: IEEE, 2023 4th International Conference on Intelligent Engineering and Management (ICIEM). P. 1—6. <https://doi.org/10.1109/ICIEM59379.2023.10166247>
- Tamrakar, P., Badholia, A. (2022). Handwritten signature verification technology using deep learning — a review. In: IEEE, 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC). P. 813—817. <https://doi.org/10.1109/ICESC54411.2022.9885550>
- Darwante, N., Sonawane, A., Suralkar, A., Pralhad, R., William, P. (2023). Hybrid model for robotic surveillance using advance computing techniques with IoT. In: 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN). P. 1301—1306. <https://doi.org/10.1109/ICPCSN58827.2023.00219>
- Chavan, P., Autade, S., Pardeshi, D., William, P. (2023). Environmental Impact of Extra High Voltage Systems in Switch Yard Transmission Lines. In: 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA). P. 1714—1718. <https://doi.org/10.1109/ICIRCA57980.2023.10220635>
- Endait, G., Nikam, A., Bhorkade, P., Lokhande, D., Agarkar, B., William, P. (2023). Hybrid model to predict leaf disease prediction using ensembling machine learning approach. In: 2023 World Conference on Communication & Computing (WCONF). P. 1—7. <https://doi.org/10.1109/WCONF58270.2023.10235119>

Sasipriya, G., Lavanya, B. (2023). Schema Design with Intelligent Multi-Modelling Computing Techniques for Health Care Applications. *In: 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. P. 1152—1158. <https://doi.org/10.1109/ICAAIC56838.2023.10140692>

Received on January 31, 2026

Reviewed on March 02, 2026

Revised on March 27, 2026

Signed for printing on April 13, 2026

Published on July 17, 2026

Рашид Бенхелуф, д-р екон. наук, кафедра економічних наук

Університетський центр Магнії

шосе Аль-Завія, 13300, Магнія, Алжир

Фатіма Зохра Бекаддур, д-р екон. наук, кафедра економічних наук

Університет Гардаї

Гардая, а/с 455b, 47000, Алжир

ПОРІВНЯЛЬНИЙ АНАЛІЗ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ І ВИПАДКОВИХ ЛІСІВ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА У ФІНАНСОВИХ ТРАНЗАКЦІЯХ

Виявлення шахрайства у фінансових транзакціях вважається критично важливим питанням, особливо з огляду на зростання кількості шахрайських дій у сучасних фінансових системах. Вивчено можливості застосування методів машинного навчання в аналізі фінансових транзакцій через залучення алгоритмів машинного навчання з учителем, заснованих на бінарній класифікації. З використанням набору даних, що містить 10 000 записів про фінансові транзакції, досліджено модель штучних нейронних мереж (ШНМ) і модель випадкового лісу. Для оцінювання продуктивності запропонованих моделей використано набір показників продуктивності, що включає точність, повноту і F1-міру. Емпіричні результати показують, що модель штучних нейронних мереж досягла точності 90,2 %, тоді як модель випадкового лісу продемонструвала вищу продуктивність з точністю 96,5 % у класифікації шахрайських транзакцій та їх відрізненні від законних.

З метою проведення порівняльного аналізу двох алгоритмів представлено основні графіки, що використовуються в статистиці для оцінювання продуктивності моделей класифікації, у тому числі ROC-аналіз, криву продуктивності та калібрувальний графік. Крім того, визначено найбільш впливові ознаки, що сприяють виявленню шахрайських транзакцій. Відповідно до цього ознаки було ранжировано так: час транзакції, день транзакції, сума транзакції, ідентифікатор транзакції і, нарешті, мерчант, що бере участь у транзакції. Результати дослідження засвідчують ефективність підходів машинного навчання з учителем у підвищенні ефективності виявлення шахрайства у фінансових транзакціях, зокрема, з точки зору досягнення високого рівня повноти й зменшення помилок класифікації.

Ключові слова: випадковий ліс; штучна нейронна мережа; виявлення шахрайства; алгоритми машинного навчання.

Надійшла 31.01.2026

Прорецензована 02.03.2026

Доопрацьована 27.03.2026

Підписана до друку 13.04.2026

Оприлюднена 17.07.2026