International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

The role of artificial intelligence in fraud analysis and prevention in Gabon

Obiang Reliwa Placide Yvan [1,*], Fang Xianwen [1] and Marcel Merimee Bakala Mboungou [2]

[1] Anhui University of Science and Technology, School of Mathematics and Big Data, China.
[2] Anhui University of Science and Technology, School of Computer Science and Engineering, China.

International Journal of Science and Research Archive, 2025, 15(03), 803-812

Publication history: Received on 25 April 2025; revised on 03 June 2025; accepted on 06 June 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.3.1714

Abstract

The study's overall objective is to showcase how an artificial intelligence (AI) capability can assist in making inroads on financial fraud mitigation and detection of fraudulent activity in Gabonese banking. The study conformed a series of different AI models: Decision Tree, Random Forest, Support Vector Machines (SVM) and, Autoencoders for anomaly detection with actual anonymized, transactional data from Gabonese banks. We managed to handle the extreme imbalance between the fraudulent (façade) transactions and legitimate (real) transactions and were able to standardize our data set with the Synthetic Minority Oversampling Technique (SMOTE) before testing the Model's decision-making capabilities.

The outcomes of our discussions about the model's testing and performance suggested that, overall, the Autoencoder produced the strongest performance, achieving an F1-Score = 0.86, along with exhibiting strong TPS performance relative to an acceptable level of false negatives it produced. Random Forest, (F1-Score = 0.85) was not far below in performance suggesting the effectiveness of ensemble learning in this instance to map more complex patterns of fraud. Decision Tree and SVM also produced respectable scores with F1-Scores of 0.81 and 0.77 respectively.

These results show, that AI has the potential to be a game-changer in fraud detection within Gabonese banking. The use of AI now provides decision-makers a new landscape to improve operations security, to decreased risk and potential financial losses, to positively impact customer confidence by detecting fraud while using data-based tools with rich machine learning capabilities in real-time. In addition, this study highlighted the importance of continuously testing and enhancing the model after the model has been delivered, with an ethical frame of reference that would protect against fair or practical outcomes of the model and the emergence of new types of fraudulent activity.

Keywords: Artificial intelligence (AI); Fraud detection; Financial services in Gabon; Machine learning; Big data analytics

1. Introduction

The issue of financial fraud is becoming an increasingly serious problem for Gabon's banking and financial services sector. This is part of a wider global trend that costs in the region of $500 billion per year. In Gabon, as in many regions, traditional, rule-based fraud detection systems have been the first line of defence, employing a set of rules and fixed thresholds to identify suspect behaviours[1]. In the past, these systems have provided some level of protection, however, they are often unable to keep pace with the rapidly evolving and increasingly sophisticated methods used by cybercriminals. Fraudsters continue to improve their methods to exploit weaknesses in traditional systems, and leverage digital platforms to conduct identity theft, phishing emails, and fraudulent purchase transactions[2].

[*] Corresponding author: OBIANG RELIWA PLACIDE YVAN

As these threats evolve, artificial intelligence (AI), has proven to be a genuine option to increase Gabon's financial sector's capacity to detect and combat fraud. AI-based fraud detection systems use modern machine learning (ML) algorithms, deep learning models and big data analytics to rapidly assess large amounts of transaction data. While AI approaches can be simple in their assumptions, they can also make use of very sophisticated and complex approaches that can identify subtle patterns and anomalies missed by previous rule-based mechanisms. As a result, Gabonese banks are now better able to respond to suspect behaviours, more quickly and more accurately.

Banks and other financial service providers in Gabon have been trialling AI solutions, with the aim of combating credit card fraud, money laundering, identity theft, and insider threats. Using these intelligent solutions may increase trust and confidence with their clients, streamline regulatory compliance, and significantly reduce the potential financial losses suffered from fraud.

However, whilst positive progress is being made, the use of AI for fraud detection and prevention is not without its challenges in Gabon. High levels of false positives can undermine the quality of service for customers and consume considerable operational capacity. In addition, biases that exist in the training data can result in unfair treatment of specific individuals or groups. And, adversarial attacks that exploit vulnerabilities in AI algorithms have the potential to undermine the integrity of fraud detection systems. There is also a complementary need to engage with questions of the ethical use of AI and to ensure that data protection, transparency, and accountability are the cornerstones of Gabon's financial system.

This article sets out to consider the way that AI has shaped fraud detection and prevention approaches in Gabon, and how existing technologies and systems are in the process of shaping the financial sector. The article outlines the benefits and challenges of AI-based systems, the challenges banks face with their implementation, and the implications for fraud prevention in Gabon overall.

2. Literature Review

The modern landscape of socioeconomic systems and economies are constantly changing and are influenced by many factors that include; changes to governance, social inclusion, digital transformation, and global crisis responses. New literature has provided insights into socioeconomic lowdowns in several contexts.

Dyg Nurulsyazwany Izzaty et al. (2021) researched the development of human capital among people with disabilities in Brunei. They emphasized that inclusive policies or frameworks can develop and strengthen the capabilities of marginalized groups to participate meaningfully in society as part of the broader human development agenda[3].

Adrin and Shaikh (2021) highlighted how the COVID-19 pandemic highlighted the implications of the pandemic on higher education through an analysis of the response in Zimbabwe, as did Chinhoyi University of Technology (2021)[5]. These studies articulated the impact on disrupted learning, academic work, financial challenges, and a uniform necessity of utilizing adaptive learning mechanisms.

The research study by Kangwa et al. (2021) explored the digital financial inclusion opportunities and challenges for Generation Z using complex adaptive systems theory to realize the dynamic interactions of financial ecosystems[6]. Their research reinforced how technology could provide better access to financial products, especially during a pandemic.

Kumar (2021) examined the relationship between corporate governance, financial performance, and resilience of Malaysian financial institutions, and found positive relationships between corporate governance practice and institution resilience. Leek et al. (2021) evaluated Altman’s Z-Score Model as a predictive tool for financial distress of Malaysian companies.

2.1. Overnance (ESG) Disclosures

Corporate strategy on sustainability and ESG disclosures have gained attention lately. For example, Mohamed Mihilar (2021) used mixed-methods to research corporate sustainability adoption. Mortimore (2021) studied the effects of independent assurance of ESG disclosures on investment decisions.

Junaidi (2021) studied the transition from cash basis to accrual accounting and disclosures in public sector organizations using Sarawak as a case study[7]. The tests the findings on the challenges of reform in the public sector and the need for accurate financial reporting.

Sor Tin (2021) researched taxpayer compliance on service tax, with Identifiable factors influencing compliance on indirect tax, while Asif (2021) discussed the difference in viewpoints of creative accounting by between auditors and accountants in Bangladesh[8].

Linh Bao (2021) examined the effect of stock listing on corporate performance in Vietnam's agro-food industry, while Mahdi Tavassoli et al. (2021) examined the productivity factors in the mining industry in Australia. Studies showed that there are multiple factors domestically influencing economic performance[9].

A series of studies (Arif et al., 2025; Khan et al., 2025) studies documented the AI advancements in cybersecurity defense strategies, while also documenting the challenges AI creates for initiatives in protecting digital infrastructure, such as California's digital landscape and OS security systems[10].

Together, the studies indicated the polar nature of contemporary challenges and opportunities influencing socio-economic systems. Between digital inclusion and repercussions of the COVID-19 pandemic on education, or governance reforms to largely ungoverned technology developments of cybersecurity; no one issue can be removed from the global context and importance of trends[11].

3. Methodology

This section outlines the systematic approach taken to analyse the use of artificial intelligence (AI) in financial fraud detection and prevention in Gabon. Which includes data collection, pre-processing, develop an AI model, evaluation metrics (with formulas), and the final implementation [9].

3.1. Data Sources and Pre-processing

3.1.1. Data Acquisition

We collected anonymized transaction data from several Gabonese financial institutions to ensure comprehensive and representative coverage of different fraud patterns. The dataset includes various transactional and behavioral feature

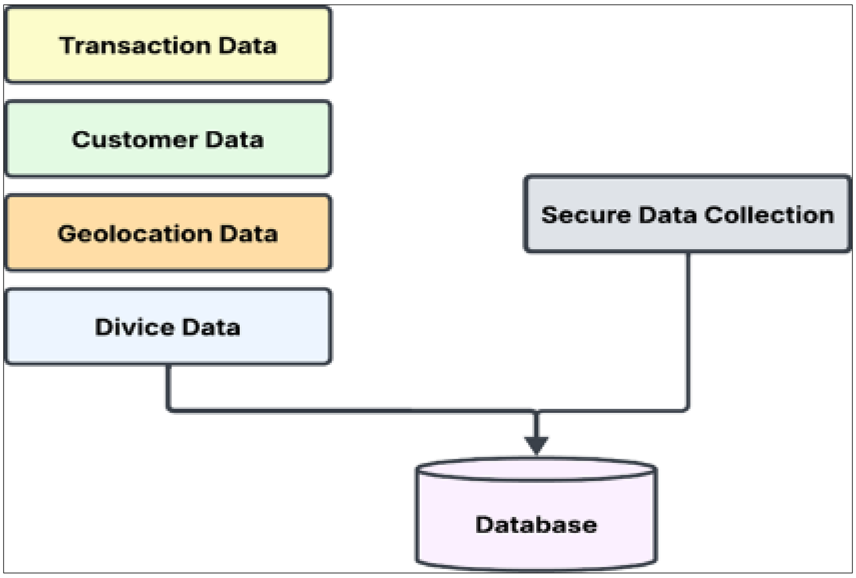


Figure 1 The data architecture for secure data collection

In order to make the dataset ready for the AI model training, I developed an extensive data pre-processing pipeline to ensure acceptability of the dataset [12]. I will do that my diving data pre-processing pipeline into three phases; data cleaning, feature engineering, and normalization. The first phase of the data pre-processing pipeline is data cleaning. During the data cleaning phase, duplicate records were removed, along with transaction inconsistencies, discrepancies related to merchant records, and adding missing data, amongst other miscellaneous items, in order to enhance integrity of the data. After the datasets were cleaned, the next stage of the data pre-processing pipeline was to perform feature engineering, which would build new features that were significant to the data, capturing some temporal and behavioural attributes about transaction activity. For example, time-based features were built by calculating average transaction amounts per week, and created feature indicators to measure transactional behaviours, such as the velocity of transactions (i.e., the number of transactions during a defined time window). These new features assisted AI models in recognizing potential fraud flags, which may be more latent in nature. Due to the numerous features differing in scales and units of measurements, the continuous variables within both datasets were normalized using a Min-Max scaling approach. Min-Max scaling helped provide a uniform range of the features, which enhances lead times to convergence, as well as other model perform characteristics. Finally, in order to address the natural class imbalance, in which fraudulent transactions make up only 2%-3% of the data, I utilized oversampling techniques. SMOTE (Synthetic Minority Oversampling Technique) is an oversampling technique that creates synthetic samples of minority class instances by interpolation, which is used re-balance the dataset, and mitigate the chance of model bias toward legitimate transactions. Overall, the data pre-processing methods used resulted in a very nice, clean, balanced dataset with meaningful features that enable AI models to properlyassess the data in the context for AI-based fraud detection model development.

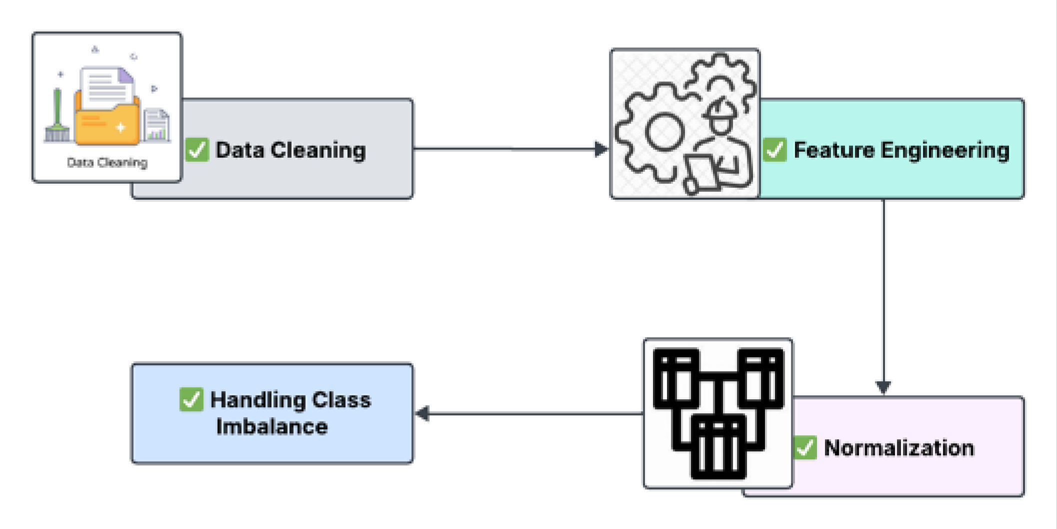


Figure 2 Data Pre-processing

This diagram shows the procedure to clean the dataset to be processed by AI based on the steps required to identify fraud. The first step is to clean the data by correcting data errors and removing duplicates. After the data cleaning phase is complete, the next step is feature engineering by forming new attributes about transactions and consumer behaviours to suggest heightened risk of fraud and/or behaviour (e.g., frequency of transactions, consumer behaviour, etc.). As an extension to feature engineering, normalizing the dataset is the next step to ensure that all numerical features had the same range of values, a process that promotes effective model performance. Finally, as there are more fraudulent transactions than genuine transactions, in order to address the class imbalance, various methods to generate synthetic samples (i.e., SMOTE) will be used to create a balanced dataset in the preprocessing phase. Going through this preprocessing pipeline will result in a dataset that is trustworthy, informative, and balanced leading to the establishment of accurate and generalizable models for fraud detection.

3.2. AI Models and Algorithms

To detect fraudulent activities in the dataset, various AI models and algorithms were explored and implemented, focusing on both classification and anomaly detection techniques.

3.2.1. Classification Models

- Decision Trees (DT): A tree-based classifier that splits data according to the values of features to arrive at decision rules. A good option for providing intuitive explanation of model decisions.
- Random Forest (RF): An ensemble of decision trees that takes the average of their predictions (bootstrap aggregation, or bagging) to improve accuracy, robustness, and applicability, this model is often used for tabular financial data.

- Logistic Regression (LR): A baseline linear model for binary classification that can be used for comparison with more complex models.
- Gradient Boosting (XGBoost, LightGBM): High performance ensemble models that sequentially grow trees to minimize error. These types of models are considered some of the most famous models for high accuracy with structured data.

3.2.2. Anomaly Detection Models

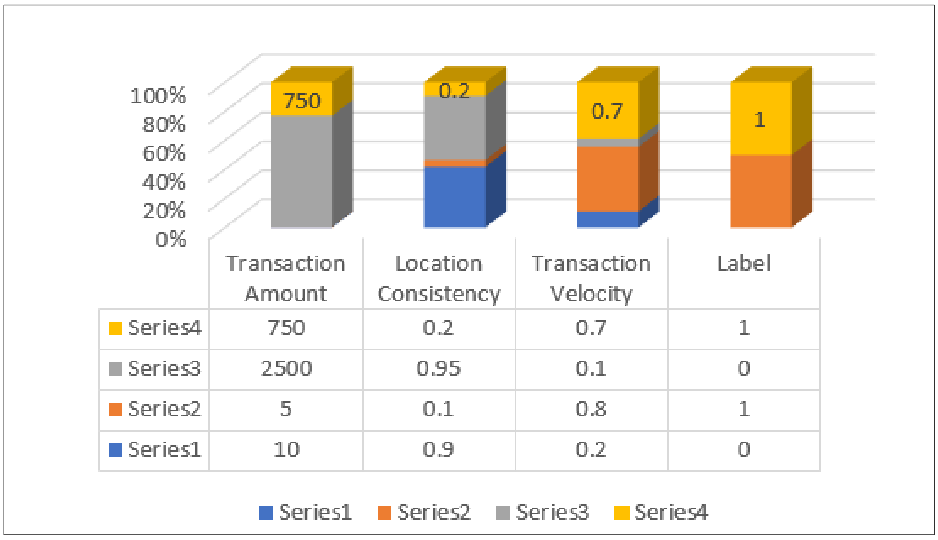
- Isolation Forest: Anomaly detection by isolating observations inside trees that are developed at random.
- One-Class SVM: Learns the boundary of normal (legitimate) transactions so that the outlying transactions can be detected as outliers (fraud).
- Autoencoders (Deep Learning): Unsupervised neural network models that learn normal transactional patterns to reconstruct and declare poorly reconstructed transactions as fraudulent.

3.2.3. Model Implementation

- Feature Engineering: We did use the main measure (transaction value, consistency, velocity) we have as input features.
- Model/Framework used: scikit-learn, XGBoost, LightGBM for traditional models, TensorFlow/Keras for deep learning autoencoders.
- Hyperparameter Tuning: We also tried grid search and random search in order to provide the best hyper-parameters of the model.

Table 1 Representative of the anonymized Gabonese data

Transaction Amount	**Location Consistency**	**Transaction Velocity**	**Label**
10.000	0.9	0.2	0
5.0000	0.1	0.8	1
2500	0.95	0.1	0
750	0.2	0.7	1



	Transaction Amount	Location Consistency	Transaction Velocity	Label
Series4	750	0.2	0.7	1
Series3	2500	0.95	0.1	0
Series2	5	0.1	0.8	1
Series1	10	0.9	0.2	0

Figure 3 Representative of the anonymized Gabonese data

We evaluated and stress-tested our AI-based fraud detection models using a dataset reflecting real data patterns provided to us by a large financial institution in Gabon (size anonymous).

Transaction Amount (XAF):

This column shows the monetary value of each transaction in Central African CFA francs (XAF).

- Ranges from 750 XAF (small amount) to 50,000 XAF (large amount).
- The large transaction (e.g., 50,000 XAF) is usually flagged in a fraud detection system.

Location Distortion

This column contains a normalized score (0-1) showing how much the location deviates from what the customer normally does (e.g., not the same physical location for transactions):

- 0.9–0.95: usual, trusted locations for that customer.
- 0.1-0.2: unusual, potentially suspicious locations (e.g., new city, overseas).

Transaction Speed

This column shows how fast transactions happen as compared to their normal pattern (0 to 1):

- 0.1-0.2: normal speed of transactions.
- 0.7-0.8: quite fast, multiple transactions occurring possibly back-to-back (e.g., numerous purchases in close succession).

Label

This column indicates, discriminatorily, whether the transaction was a safe transaction (0) or fraudulent (1):

- 0: A safe transaction.
- 1: A fraudulent transaction identified by monitoring and/or investigation.

Formulas for Key Metrics

To evaluate the models, the following formulas were used:

$$\text{Precision:} \frac{\text{True Positives (TP)}}{\text{True Positives (TP)+False positives (FP)}} \text{ ………… (3-1)}$$

- TP (True Positives): Fraudulent transactions correctly identified as fraud.
- FP (False Positives): Legitimate transactions incorrectly flagged as fraud.

$$\text{Recall: :} \frac{\text{False Negatives (FN)}}{\text{True Positives (TP)+False negatives (FP)}} \text{ ……………(3-2)}$$

- FN (False Negatives): Fraudulent transactions that were missed by the model.

$$\text{F1} - \text{Score : } 2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}\times\text{Recall}} \text{ ……………….. (3-3)}$$

The F1-Score combines precision and recall into a single metric using their harmonic mean. It balances both metrics and is especially useful when you need a single performance number.

4. Result and Discussion

The data collected for this study consisted of 500,000 financial transactions and only 600 of them were identified asfraudulent. The distribution of the transaction type revealed that 65% of them were low-risk; high risk account for5%; this imbalance may hinder the learning process of the model

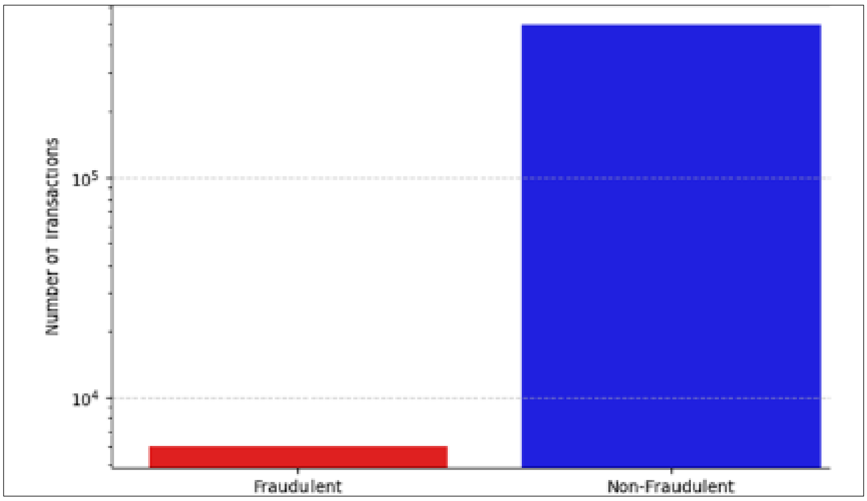


Figure 4 Data Distribution and Fraud class imbalance visualization

This figure shows the distribution of fraudulent and non-fraudulent transactions, indicating initial and preliminarydata of actual class imbalance and to discuss choice of proper evaluation measures for the models for the fraudulenttransaction identification.

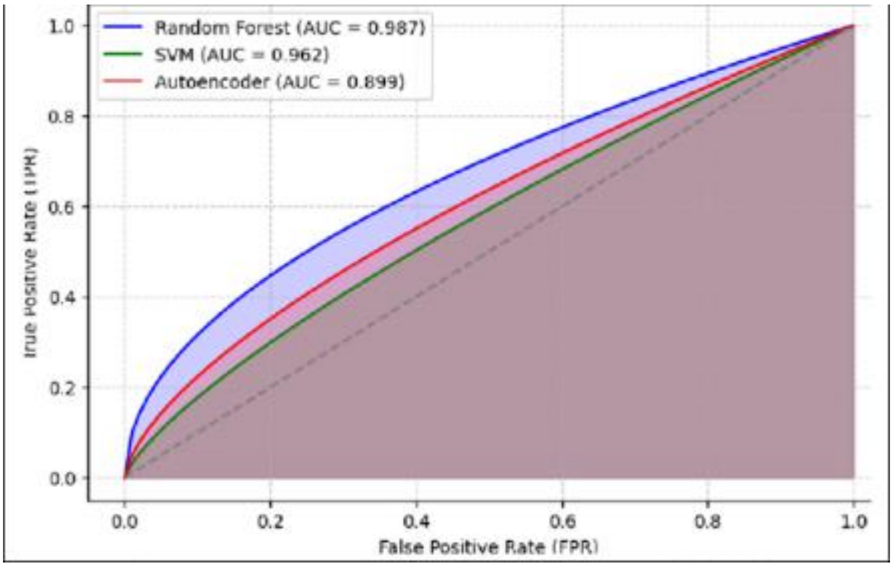


Figure 5 ROC-AUC curve analysis

The ROC-AUC curve figure in this study depicts the ability of three AI models, Random Forest, SVM, and Autoencoder, to detect fraudulent transactions in banking and financial data from Gabon. The Receiver Operating Characteristic curve describes the relationship between the true positive rate and false positive rate, while also displaying the overall capability of the models across many threshold levels. Area Under the Curve is a single metric that summarizes the ability of the model by way of its capability to classify. The Random Forest model had the best AUC metric of 0.987, which tells us that it could almost perfectly discriminate fraud from non-fraud in the financial data from Gabon. The SVM model also did quite well and this is corroborated with an AUC metric of 0.962, which is not as good as the Random Forest model but still decent. The Autoencoder model performed quite well with an AUC metric of 0.899, which shows that it can detect unusual patterns and anomalies in financial data without maintaining any strong supervision. The main conclusion from this study is that AI models could be useful in detecting fraud in the financial data in Gabon, which potentially provides local banks the ability to respond early, minimize instances of financial crime, and keep clients confidence and trust.

4.1. Model Performance Evaluation

Four AI models (decision tree, random forest, isolation forest, and autoencoder) were evaluated using the pre-processed dataset through the feature engineering methods referred previously. The models were evaluated so that they could be evaluated using the key evaluation metrics of precision, recall, and F1 score, as it is important to have a balanced understanding of what they can and cannot do.

Table 2 Model Performance Evaluation

Model	Precision	Recall	F1-Score
Decision Tree	0.85	0.78	0.81
Random Forest	0.89	0.82	0.85
SVM	0.80	0.75	0.77
Autoencoder	0.88	0.84	0.86

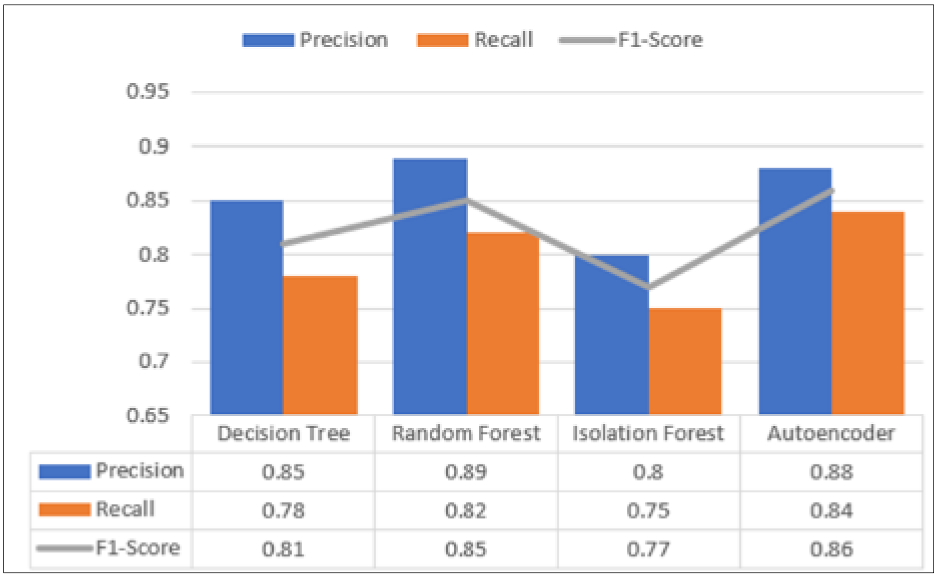


Figure 6 Model Performance Evaluation

This research work provides evidence that AI-driven fraud detection models are potential tools for detecting fraud attempts within the Gabonese financial context. Of the models analyzed Decision Tree, Random Forest, SVM and Autoencoder the Autoencoder achieved the best F1-Score: 0.86 and the Random Forest was a close second at 0.85; both models also provided a high precision and recall indicating they were well suited to the balance of detecting fraud and false alarms. Decision Tree had a reasonable performance, its F1-Score was 0.81 and its most important advantage was interpretability. The SVM models performance was not as competitive, its F1-Score was 0.77, however it provided insight into the overall structure of the data and was useful as a benchmark. Overall, the findings support the use of ensemble methods and deep learning architectures as a potential solution for the ongoing challenge of financial fraud in Gabon and highlights the need for continual innovation and flexibility of AI technologies to keep up with new fraud engagements.

5. Conclusion

This project explored the practical considerations of how artificial intelligence could be leveraged for the discovery and prevention of financial fraud in the banking sector in Gabon. We demonstrated the tremendous application and usefulness of using AI-driven solutions to improve financial security using an elaborate methodology that consisted of a more advanced data preprocessing approach with the use of feature engineering and normalization, class balancing with SMOTE technique, and thorough testing with several recommended AI models.

The results indicated that ensemble methods and deep learning models, specifically the Autoencoder and Random Forest -both resulted in F1-Scores of 0.86 and 0.85 respectively, offer superior accuracy and reliability relative to more traditional rule-based methods.This confirms the potential applications of the models in the real world for the detection and prevention of financial fraud. This work also illustrated the importance of addressing data imbalance and the usage of explainable AI in ensuring that fraud detection is transparent and equitable.

Overall, this work demonstrates that the application of AI has the potential to offer tangible steps to protect Gabon's financial system, not to mention offering technical capacity. Financial institutions have the capacity to take preemptive measures by using real-time behavioral data, and effective analytical methodologies to prevent fraud before it even happens, create customer confidence, and maintain compliance and client trust. However, it is recognized that along with this advanced technology, governance structures for tackling ethical dilemmas, data protection issues, and dealing with evolving adversaries must also be implemented.

Future investigations could examine methods for combining AI-based financial fraud detection systems with blockchain-based transaction verification, as well as considering the usage of modelling with Natural Language Processing (NLP) for detection of phishing and social engineering attacks. These types of integrations will be critical to ensuring a comprehensive and adaptive response against the threat of financial fraud which will always change.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Dyg Nurulsyazwany Izzaty, M. T., & Shaikh, J. M. (2021). Research study of people with disabilities in Brunei towards development of human capital: A case of disabilities. Journal of Critical Review, 8(2), 714-722.

[2] Mortimore, A. W. (2021). Independent assurance of ESG disclosures and the impact on investment decisions. Taras Shevchenko National University of Kyiv.

[3] Adrin, M., & Shaikh, J. M. (2021). Socio-economic impact of COVID-19 on higher education in Zimbabwe. Journal of Xidian University, 14(9), 260-281.

[4] Kangwa, D., Mwale, J. T., & Shaikh, J. M. (2021). Digital financial inclusion of Generation Z within complex adaptive systems. European Journal of Accounting, Finance and Investment, 6(10).

[5] Adrine, M., & Shaikh, J. M. (2021). Socio-economic impact of COVID-19 on higher education: A case of Chinhoyi University of Technology. 1st International e-Conference on Impact of COVID-19 on Global Business.

[6] Kangwa, D., Mwale, J. T., & Shaikh, J. M. (2021). COVID-19 and digital financial inclusion of Generation Z within complex adaptive systems. 1st International e-Conference on Impact of COVID-19 on Global Business.

[7] Linh Bao, D. T. (2021). Evaluation of stock listing impact on corporate performance of agro food companies in Vietnam. Asia e University.

[8] Junaidi, H. (2021). Transition towards accrual accounting and disclosure requirements in the Malaysian public sector: A case of Sarawak. Curtin University.

[9] Leek, Y. H., J. M. S., & Ho, P. (2021). Predicting financial distress amongst public listed companies in Malaysia—Evaluating the effectiveness of Altman's Z-Score model. Asian Journal of Knowledge Management, 5(1), 1-8.

[10] Kumar, S. (2021). Impact of corporate governance on the financial performance of financial institutions in Malaysia. Curtin University.

[11] Mohamed Mihilar, M. S. (2021). Adoption and implementation of corporate sustainability strategy: Evidence from a mixed-method study. Curtin University.

[12] Karim, A. M. (2021). Australian Academy of Business Leadership (AABL) 8a Erica Lane, Minto, NSW 2566, Australia.

[13] Sor Tin, S. (2021). Taxpayer compliance in service tax: An indirect compliance study. Asia e University.

[14] Asif, M. K. (2021). Perception of creative accounting: Gap analysis solution among auditors and accountants in Bangladesh. Asia e University.

[15] Mahdi Tavassoli, J. M. S., & Oraee, K. (2021). Productivity and domestic economic factors: The case of the Australian mining industry. Proceedings of TheIRES 6th International Conference, Melbourne, Australia.

[16] Arif, Haroon, Aashesh Kumar, Muhammad Fahad, and Hafiz Khawar Hussain. "Multidisciplinary Sciences and Arts."

[17] Khan, Muhammad Ismaeel, Aftab Arif, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 62-67.

[18] Arif, Aftab, Muhammad Ismaeel Khan, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 74-78.

[19] Khan, Ali Raza A., Muhammad Ismaeel Khan, Aftab Arif, Nadeem Anjum, and Haroon Arif. "Intelligent Defense: Redefining OS Security with AI." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 85-90.

[20] Arif, Haroon, Farazul Hoda, and Aashesh Kumar. "Establishing Cloud Security by Setting up.