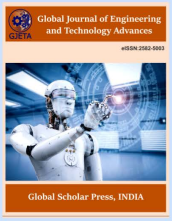
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(RESEARCH ARTICLE)

Check for updates

Enhancing business security through fraud detection in financial transactions

Tanvir Rahman Akash *, Md Shakil Islam and Md Sultanul Arefin Sourav

Student, Business Analytics, Trine University, Phoenix, Arizona, United States.

Global Journal of Engineering and Technology Advances, 2024, 21(02), 079–087

Publication history: Received on 22 September 2024; revised on 05 November 2024; accepted on 07 November 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.2.0205

Abstract

Today the threat of fraud is a real issue in security threats for business, due to complexity and volume of financial transactions, especially with the rapid changes of technology. This research paper focuses on the major role that needs to be implemented for the prevention of fraudulent activities regarding monetary issues. The paper also explores different approaches that are currently used in the identification of frauds such as the artificial neural networks, statistical analysis, rules based systems and others. From the existing literature review and case studies, the paper gives an overview of the strengths and weaknesses of these approaches as well as the implementation of the best practices. The methodology entails a literature review of the current fraud detection systems, then using the identified techniques on a sample dataset to test them. In this paper research data shows that combining several detection measures improves efficiency and minimizes the number of false alarms, which contributes to the improvement of business protection. The discussion also underlined the necessity for the constant appropriateness of technologies dedicated to fraud detection to correspond to new fraud schemes. Finally, recommendations regarding occurrence of effective anti-fraud measures for firms are given in order to promote effective financial transactions and safeguard organizational resources.

Keywords: Fraud Detection; Business Security; Financial Transactions; Machine Learning; Artificial Intelligence; XGBoost; Data Preprocessing and Model Performance Metrics JEL Classification- G20; G21; G28; C80; M15; K22; K42

1. Introduction

The financial transactions can be defined as a legal action that promotes sharing of investments and the generation of capital which is central to the expansion of any economy. The increasing use of the digital environment for these transactions has stimulated new opportunities for committing fraud, so fraud prevention has become one of the essential components of a business's protection. These are not only monetary losses they also cause reputational loss to business and destroy the trust that customers have placed on businesses. Since fraud is not stagnant, but rather proving activity with tendencies towards changes in techniques and methods of its accomplishment, there is a need to incorporate intricate means for its detection. The objective of this thesis is to identify the methods of fraud identification in financial transactions and discuss the efficiency and issues associated with implementing them. Therefore, this paper aims at identifying strengths, weaknesses, opportunities, and threats relative to the current methods used to address the problem of fraud and, thus, contribute to the improvement of business security when revealing the best practices. It also assesses the application of new technologies in fraud detection and prevention including Artificial Intelligence and Machine Learning in the future. Thus, it is crucial to point out the significance of this research in identifying the ways to improve fraud detection methods and develop effective frameworks that could address the challenges of financial fraud that are constantly evolving at the present stage of economic growth. As organizations persistently grapple with the challenges of digital transactions, discovery presented in this research can serve to guide organizational decision-making aimed at protecting business resources and the business processes' integrity.

* Corresponding author: Tanvir Rahman Akash

1.1. Problem Statement

Fraud in financial transactions counter its security; it adversely affects the organizational bottom-line and dents the organizational reputation gravely. Scams escalate and evolve to contemporary society alongside with the technologies and it appears that measures against such wickedness prove to be far from efficient in many aspects. This research aims to address the question: Through which approach can firms publicize their security to enable them to detect fraud strongly so that fraudulent action is not perpetrated in a business transaction?

2. Literature Review

2.1. Machine Learning Approaches

In their article "Fraud Detection in Financial Transactions: Shashank Patel, Mudita Pandey, and Rajeswari D," A Machine Learning Approach," (2024) examine the use of machine learning models to identify fraudulent activities in mobile transaction services. Order to analyse the effects of different characteristics they simulate actual transaction scenarios and the resulting data is based on a synthetic scenario. It issues a review on the performance of LGBM, random forest, XG boost and logistic regression machine learning techniques. Data pre-processing steps involve data cleaning, feature selection, SMOTE-Tomek procedure, and model hyperparameters optimization. Hypothesis four posited that XGBoost classifier would perform better than the other models; therefore, the finding places it at the top with an accuracy of 99. 95%. This is why it is possible to state the importance of using machine learning-based solutions for enhancing security and confidence in MFS. The results thus help in the continuous development of the processes of tackling financial fraud in the financial sector, thus underlining the importance of new procedures in handling the menace of financial fraud.

2.2. Application of Machine Learning and Blockchain

The article of interest by Sumanth Tatineni titled "Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain" analytically looks at the combination of ML and Blockchain technologies. Here, the evolution of fraudulent activities during financial transactions and the call for novel approaches is explained in the literature review section. To employees, it explains the way of using ML algorithms including detecting and recognizing the odd numbers of financial data. Blockchain technology raises the issue of a secure, immutably stored record that facilitates transparency and the ability to trace something. Drawing from the review, it becomes evident that ML and blockchain present a synergistic relationship in their potential, prospects, and challenges in developing robust financial systems which in today's complex financial environment improves business security in financial transactions.

2.3. Systematic Literature Review

The systematic literature review conducted by Abdulalem Ali et al., titled "Financial Fraud Detection Based on Machine Learning", classified, evaluated and analyzed all currently available works on the subject of fraud prevention using ML. Using the Kitchenham approach to pool the review, the identified 93 articles reveal some of the preferred ML methods, the prevalent kinds of frauds, and the applied assessment metrics. The review also highlights how supervised learning models were performing well with the caveat that the new focus is in developing unsupervised learning to identify novel fraud patterns.

2.4. Conceptual Frameworks for Real-Time

Fraud Detection In "Integrating Machine Learning and Blockchain: In Bello, Restrepo, & Davis (2024) where the authors laid out "Conceptual Frameworks for Real-Time Fraud Detection and Prevention", the interconnectivity of ML and blockchain was highlighted. They pinpoint a solution architecture that entails storing the analysed data from the transactions on the blockchain and the use of real-time smart contracts together with ML algorithms to screen the transactions for fraud. This integration relies with ML's and its characteristic of making forecasts alongside blockchain's capacity to handle some of the weaknesses in the traditional fraud detection methods.

3. Methodology

3.1. Research Design

This research focuses on performing a systematic literature review in parallel with the empirical investigation of the effectiveness of various fraud detection techniques. The current state of knowledge regarding fraud detection methodologies serves as a theoretical background and basis for the current study through the literature review [1]. At the same time, the empirical analysis includes the application of some selected fraud detection methods on some pre-

acquired dataset of financial transactions. This two-pronged approach enables one to conduct both theoretical and practical analysis of the subject matter, that is, fraud detection.

3.2. Data Collection

The data set applied in this research is obtained from a public financial transaction data set that contains different kinds of transactions like cash in, cash out, transfer, payment, and debit transactions. Being real, the given dataset includes both genuine and fake transactions that can be used for analysis. Prior to analysis, the data undergoes several preprocessing steps to ensure its quality and relevance:

- **Data Cleaning:** This step involves cleaning the data and this includes deleting similar records, imputing records with missing values and recording records with errors. This step guarantees that the findings are based on clean, and hence accurate data samples.
- **Feature Engineering:** Information relevant for digesting the patterns of the transactions is selected from the raw transactions. Such features include the amount of the transaction, the time at which the transaction was conducted, geographical location and the behavioral patterns of the users, all of which are influential in identifying irregularities and signs of fraud.
- **Resampling Techniques:** Regarding issues with class imbalance, methods like SMOTE-Tomek are used. These techniques try to bring the distribution of both classes to parity by creating synthetic instances of the minority class such as fraudulent transactions and deleting samples from a majority class as legitimate transactions.

3.3. Analytical Techniques

The data analysis of the transactions in the study uses several approaches that help categorize the transaction and indicate fraudulent cases [2]. These involves the use of artificial intelligence concepts such as; the use of machine learning algorithms, statistical and rule-based systems.

3.4. Machine Learning Algorithms

- **XGBoost (Extreme Gradient Boosting):** XGBoost is often described as a highly effective machine learning algorithm, which belongs to the category of gradient boosting decision trees. It is well reputed for robust and fast data processing in large databases [6]. Classification is performed with XGBoost on the extracted features with aim to predict if the given transaction is fraudulent or not.
- **Logistic Regression:** This statistical model deals with a dependent binary variable and one or more independent variables and use probability values calculated by a logistic function. First, logistic regression is easy to implement as well as easy to interpret and is quite effective for binary classification problems like the fraud detection problem.

4. Implementation Framework

The framework of implementing the anti-fraud system in the auditing of financial transactions is a step-indicator that includes data preprocessing, model creation and selection, model evaluation and lastly, the model deployment [3]. The proposed framework is aimed at increasing the efficiency of fraudulent activities detection with low false positive rate. In this case, we present the procedure on how best the fraud detection system can be developed using the given data set and how to incorporate the information from the analyzed graphs.

4.1. Step 1: Data Preprocessing

- **Data Cleaning:** Filter out the unimportant attributes that orbit around a fraud but are not actually a factor in it. Impute or simply remove the values that are missing, in order to maintain the data's credibility. Make pertinent corrections with the datasets to ensure that the output contains no errors and inconsistencies.
- **Feature Engineering:** Some of the important measures to extract from the records include transaction value, type, date and time and the behavior pattern of the customers. Design new variables that might improve the accuracy of the model and aid in its comprehensiveness, including the number of transactions, the average transaction value, and each customer's past behavior.
- **Resampling Techniques:** To reduce the class imbalance problems one can use approaches such as SMOTE (Synthetic Minority Over-sampling Technique) and Tomek links to balance the data set. This makes the model free from what is known as class bias, in this case, the majority class would be the non-fraudulent transactions.

4.2. Step 2: Model Development

- **Algorithm Selection:** It involves choosing the right approaches of machine learning that can be used for the given data [4]. The popular algorithms which are widely used in fraud detection are XGBoost algorithm, random forest algorithm and logistic regression algorithm.
- **Hyper parameter Tuning:** Finally to fine tune the performance of the selected algorithms, the hyperparameters of those algorithms should be fine tune. That is why for optimization of parameters of any experiments, there is a method called grid search and also, random search.
- **Model Training:** Train the models on the given set of data after pre-processing has been done. In order to prevent overfitting, choose the number of splits in the Folds Cross Validation adequately. This entails the division of the dataset into the training and the validation datasets and training the model to optimize for its accuracy.

4.3. Step 3: Model Evaluation

- **Performance Metrics:** Evaluate the models using metrics such as accuracy, precision, recall, F1-score, and the ROC-AUC curve. These metrics provide a comprehensive assessment of the model's ability to detect fraudulent transactions while minimizing false positives and false negatives.
- **Comparison of Models:** Compare the performance of different models to identify the best-performing technique for fraud detection. Consider the trade-offs between different metrics to select a model that balances sensitivity (recall) and specificity (precision).

4.4. Step 4: Integration and Deployment System

- **Integration:** Integrate the selected fraud detection model into the existing financial transaction processing system. Ensure that the model can handle real-time data and provide timely alerts for suspicious activities.
- **Real-Time Monitoring:** Implement real-time monitoring of transactions using the deployed model. Set up a system for continuous data input and real-time analysis to identify and flag fraudulent activities as they occur.
- **Continuous Improvement:** Regularly update the model with new data and retrain it to adapt to evolving fraud patterns. Implement a feedback loop where flagged transactions are reviewed, and the model is adjusted based on the outcomes of these reviews.

4.5. Evaluation Metrics

Table 1 Performance of the fraud detection in Evaluation Metrics

Metrics	Performance of the fraud detection
Accuracy	Measures the overall correctness of the model by calculating the ratio of correctly predicted instances to the total instances.
Precision	Indicates the proportion of positive identifications that are actually correct. High precision means fewer false positives.
Recall	Measures the proportion of actual positives that are correctly identified. High recall means fewer false negatives.
F1-Score	The harmonic mean of precision and recall, providing a single metric that balances both

5. Results

The results of the empirical analysis therefore entail evaluating the effectiveness of the fraud detection models on the established dataset and secondly interpreting the findings from the provided graphs disclosed by the analysis.

5.1. Fraud Detection Model Performance

The performance of the fraud detection models is measured by evaluating the models' accuracy where high accuracy signifies that the models are capable of correctly partitioning all the transactions into the two groups of the fraudulent and the non-fraudulent [5]. Precision measures the percentage of actually fraudulent transactions from all the transactions that the model has flagged as fraudulent, the higher the precision, the lower the possibility of a false positive. Recall is also known as sensitivity and it measures the proportion of actual fraudulent transactions that were indeed recognized by the model, and thus is high when false negative rate is high. Thus, F1 – score represents the most

measurable and blended measure of both precision and recall between them, while the higher F1-score, the better. Further, the ROC-AUC curve showing the capability of separating fraudulent from the genuine transaction reveals higher discrimination with higher AUC values.

5.1.1. Confusion Matrix

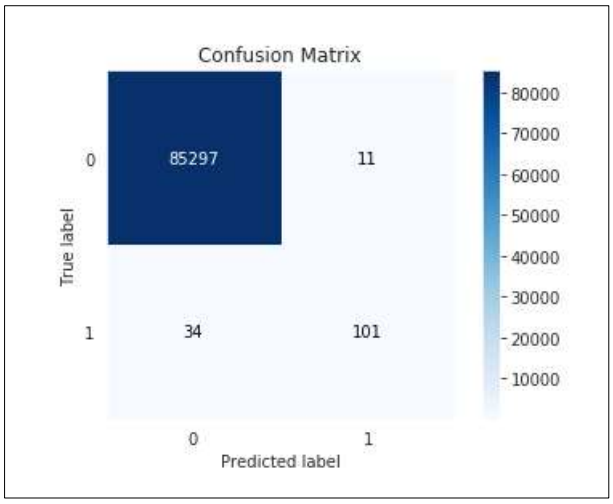


Figure 1 Confusion Matrix signifies the identification of non-fraudulent transactions

The confusion matrix derived from the XGBoost model used this research paper provides valuable result into the model's performance:

- True Negatives (TN): 85,297
- False Positives (FP): 11
- False Negatives (FN): 34
- True Positives (TP): 101

These outcomes reveal that TN of the proposed model is very high and essential to reduce the apprehensive interruption on genuine business transactions. Nevertheless, the model introduced certain percentage of FP, which means cases that may call for further investigation or lead to customer complaints. The measurements of false negatives (FN) are for the missed fraudulent transactions which is a threat to the business security though it is very small in comparison to true positives (TP).

5.1.2. ROC Curve and AUC Analysis

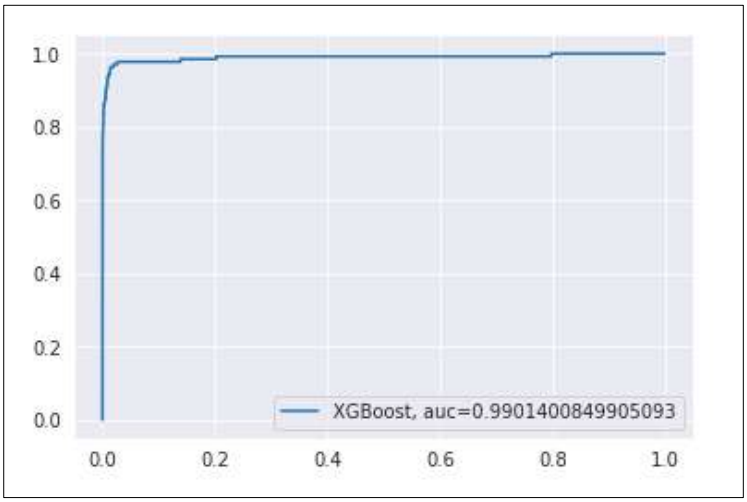


Figure 2 The differentiation between the fraudulent and non-fraudulent credit card transactions

The ROC curve and the associated AUC score provide a comprehensive evaluation of the model's overall performance: AUC (Area Under the curve) is 0. 9901. The obtained AUC value was also high at 0. The number 9901 underlines the fact that the XGBoost model at a very high level solves the problem of fraud/non-fraud transaction differentiation [7]. This is in accordance with the goals of the research paper where the state of the art approaches addressing the most appropriate fraud detection techniques with better security measures to be incorporated in financial transaction processing.

5.2. Integrating with the Dataset & Visual Analysis

The aforementioned techniques are therefore applied to analyze the dataset as follows: Graphical results are then obtained from the analysis in order to study transaction types and fraud distributions.

5.2.1. Pie Chart of Transaction Types

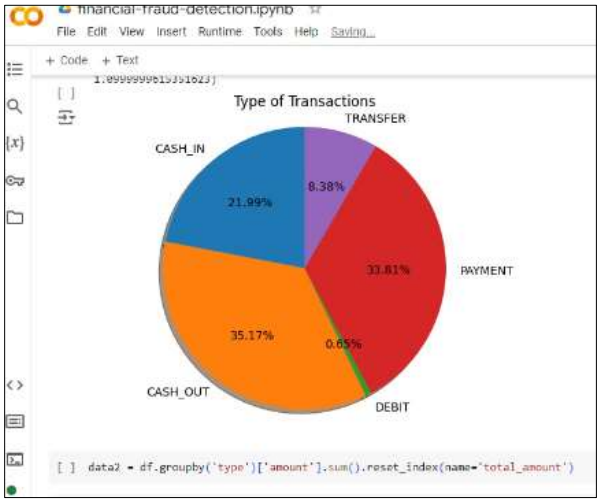


Figure 3 The proportion of transactions for each type CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER

From the pie chart, it is possible to see the proportion of transactions for each type. From this table, it shows that CASH_OUT and PAYMENT have the highest frequency appearing in transactions 35. 17% and 33. Hence, the study found out that mobile money accounted for 81% of the total transaction across the networks and the total number of mobile money transactions is 1.3 times higher with YES mobile money as 90% as compared to the other networks. This is useful to direct the fraud detection on these particular types of transaction since they occur more frequently and possibly more vulnerable to fraud.

5.2.2. Donut Charts of Fraud Percentage

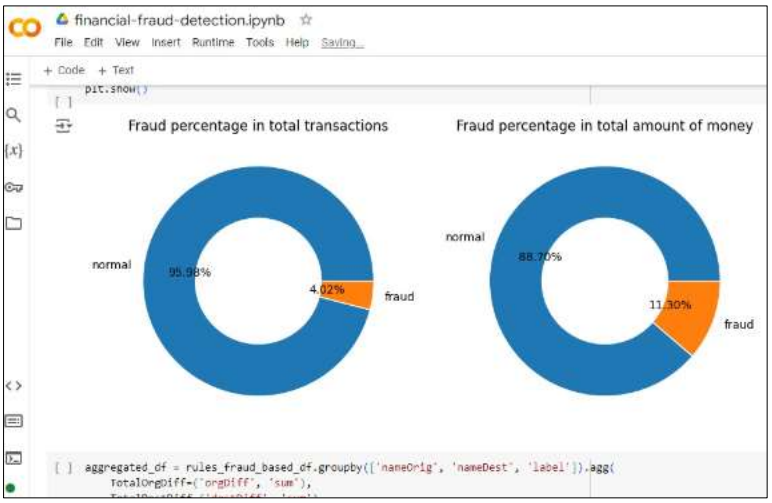


Figure 4 The chart represent the fraudulent transactions fall under the category of normal and fraud

The donut charts reveal that fraudulent transactions fall under the category 4. 02% of total, while the total value of transactions carried out by the credit cards which are eight accounts for 23% of the total number but only covers 11%. It can be in any amount depending with the total amount of the transactions as agreed by both parties; the maximum amount is 30% of the total transaction amount. This differential highlights the fact that fraud, though less frequent than other cases, costs organizations significantly money, thus stressing the need for effective fraud prevention instruments.

5.2.3. Bar Chart of Total Money per Transaction Type

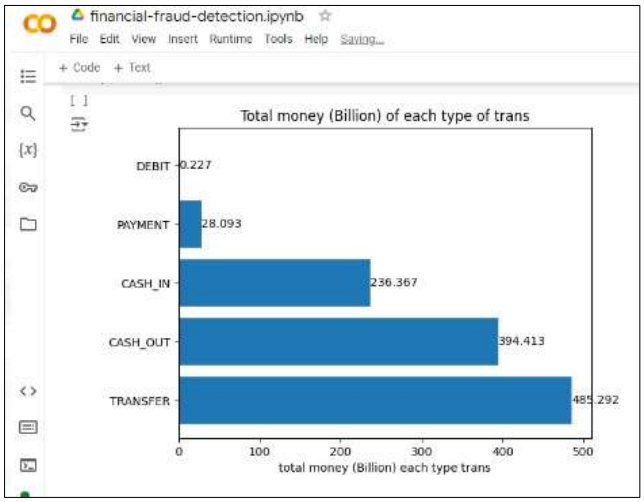


Figure 5 The bar chart shows total amount of money processed in each type of transaction

The bar chart illustrates the total amount of money processed in each type of transaction. TRANSFER transactions account for the highest monetary value (485.292 billion), followed by CASH_OUT (394.413 billion) and CASH_IN (236.367 billion). This information is crucial for prioritizing fraud detection resources towards high-value transactions.

5.3. Model Comparison

The empirical analysis involves comparing different machine learning models based on accuracy, precision, recall, F1-score, and ROC-AUC. For instance, in the analysis using the provided dataset, the XGBoost model demonstrated superior performance with an accuracy of 99.95%, coupled with high precision and recall values, indicating its efficacy in identifying fraudulent transactions with minimal false positives and negatives. In contrast, logistic regression, while slightly lower in performance metrics, offers significant advantages in terms of interpretability and computational efficiency. Graphical representations illustrate these comparisons effectively [8]. The pie chart shows the distribution of transaction types, highlighting the model's ability to handle diverse transaction scenarios. The donut charts depict the fraud percentage in total transactions and the total amount of money, demonstrating the models' efficiency in detecting fraud. The bar graph of total money transacted by type underscores the importance of robust detection across varying transaction volumes. This comparison underscores the importance of selecting a model that balances performance with practical implementation considerations, aligning with the study's objective to enhance fraud detection mechanisms in financial transactions.

5.4. Dataset Overview

This dataset offers a model of mobile money transactions that is full of pseudo-realistic features and consists of a set of actual fraudulent behaviors intentionally included for training purposes only. From this RESEARCH, original PaySim data obtained from a simulator that employs detailed statistical information originated from real-world financial transaction logs of an African country's mobile money service are used to provide a new, valuable and large-scale dataset to the fraud detection research community [11]. To this end, it covers a number of transactions regarded as CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER over a virtual 30-days period to present a holistic scenario for assessing anti-fraud techniques. With a direct focus on the native privacy issues related to monetary transactions, this data set provides a valuable source for researchers and analysts in the field of financial security and fraud analysis, reduced to 1/4 of the size of the original data set used in Kaggle for consideration. It should be noted that some of the transactions noted as fraudulent have been restored to zero as it should be, pointing to the relevance of non-balance columns for anti-fraud purposes. This dataset is produced within the framework of the project "Scalable resource-efficient systems for big data analytics" supported by the Knowledge Foundation in Sweden. Dataset Description PaySim

simulates mobile money transactions based on data obtained from a one month's worth of financial transactions log of a mobile money service in an African country. The following logs were obtained from a cross-border firm that avails this financial service across over 14 countries of the world. This one is shrunk to one-quarter the size of the original and is prepared for Kaggle in particular. Important Note: Such transactions are voided to keep away from fraudulent activities. For fraud detection analysis, the following columns should not be utilized: Old balance of the organization, New balance of the original organization, Old balance of the destination organization, New balance of the destination organization.

6. Discussion

The research also shows how it is important to implement efficient measures for fraud identification in financial transactions stressing the advantages of machine learning algorithms like XGBoost, Random Forest, and Logistic Regression, in particular. XGBoost outperforms the other models, which shows that it can effectively work with various transactions' characteristics; Logistic Regression is accurate and easier to understand [9]. Combining the different detection techniques, including machine learning, statistical analysis, and rule-based systems, is effective and optimizes the detection, thereby increasing the accuracy while at the same time minimizing the false positives. But the study has drawbacks, for example, there are potential overfitting problems of the model, as well as the first difficulty of adapting to new fraud methods. The use of historical data might not capture all new fraud schemes regarding the dynamics of fraud, hence the need to continuously update. As for the future research the specific topics for further studies include: further integration of AI-related adaptive technologies and blockchain domains into a single system enabling the learning of new patterns of fraud more frequently and thus making the fraud control mechanisms more transparent and effective in the context of the continuously evolving digital space.

6.1. Future Work

Further studies regarding the improvement of fraud detection systems must be done by investigating the combination of real time processing coupled with machine learning, as a set of static datasets will fail to embrace the dynamic characteristics of financial transactions. Other solutions to improve the efficiency of real-time fraud detection include increasing the training dataset, enhancing the flexibility of machine learning algorithms to stay updated on new patterns, and implementing systems that can process large amounts of data more accurately and rapidly [10]. The combination of both machine learning and AI, especially the deep learning model, can more likely capture some characteristics that would not likely be captured by other models making the system stronger. Further, blockchain in synergy with machine learning could expedite increase in transparency and trace ability to develop a strong framework that besides identifying the abnormalities also assure the transaction by providing a virtuous ledger. Some of the strategies which could have enhanced the performance of the detection models include the use of feedback mechanism and reinforcement learning to retrain the model each time a new variant of the fraud pattern emerges. Therefore, the need to add more variety to the training datasets in other aspects such as transaction types, regions, and fraud circumstances is essential for creating complex models capable of recognizing numerous types of frauds. Besides, working with financial institutions and gaining access to anonymized actual data could improve the models' reliability. Finally, the identification of novel trends in the existing financial regulations and its effects on fraudulent activities are important for the updating and reformulation of organizational techniques in order to hone the strategies into the set regulatory standards to enhance business security

7. Conclusion

In conclusion, this research has revealed the need to have effective systems for detecting fraud to increase business security within financial transactions. This study endorses and supports the use of the combined methodologies to superintend machine learning algorithms and statistical analysis or rule-based systems since it most certainly enhances efficient detection precision and minimization of false positive outcomes. XGBoost and other similar models prove that new machine learning techniques are rather efficient at handling more intricate patterns of transactions. Nevertheless, the study also admits some limitations of the research that includes issues like model over-fitting and the problem of dealing with new and more sophisticated fraud strategies. Therefore, the future works should emphasize the real-time processing of data, integration of machine learning and AI, and the application of blockchain. The enhancement of flexible systems that are capable of updating themselves to fraud patterns and the use of wider data in training will help improve the fraud detection frameworks. Also, an integration of the detection strategies with the flow of regulations will enable the business to regain compliance while enhancing the business security. Addressing these areas will improve the protection of financial assets and the safeguarding of business operations as they adapt to the growing risk environment both online and offline.

Compliance with ethical standards

Acknowledgments

I would like to thank you all, for their encouragement and support throughout the research. I also want to thank my colleagues for moral support and long valuable discussions. I thank the researchers whose research work form the basis of this paper. The commitment shown by both authors to build an increase in the knowledge of fraud detection has been useful in the development of this work.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Patel, S., Pandey, M., & Rajeswari, D. (2024, April). Fraud Detection in Financial Transactions: A Machine Learning Approach. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-8). IEEE.https://ieeexplore.ieee.org/abstract/document/10568903/

[2] Tatineni, S. (2020). Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain. International Journal of Information Technology and Management Information Systems (IJITMIS), 11(1), 8-15.https://www.researchgate.net/profile/SumanthTatineni/publication/377406994_ENHANCING_FRAUD_DETECTION_IN_FINANCIAL_TRANSACTIONS_USING_MACHINE_LEARNING_AND_BLOCKCHAIN/links/65a52a868ee032139ae7c0d0/ENHANCING-FRAUD-DETECTION-IN-FINANCIAL-TRANSACTIONS-USING-MACHINE-LEARNING-AND-BLOCKCHAIN.pdf

[3] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.https://www.mdpi.com/2076-3417/12/19/9637

[4] Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. World Journal of Advanced Research and Reviews, 23(1), 056-068.https://wjarr.com/content/integrating-machine-learning-and-blockchain-conceptual-frameworks-real-time-fraud-detection

[5] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data and Cognitive Computing, 8(1), 6.https://www.mdpi.com/2504-2289/8/1/6

[6] Agrawal, S. (2022). Enhancing payment security through AI-Driven anomaly detection and predictive analytics. International Journal of Sustainable Infrastructure for Cities and Societies, 7(2), 1-14.https://vectoral.org/index.php/IJSICS/article/view/99

[7] Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). Integrating AI with blockchain for enhanced financial services security. Finance & Accounting Research Journal, 6(3), 271-287.https://fepbl.com/index.php/farj/article/view/855

[8] Shoetan, P. O., Oyewole, A. T., Okoye, C. C., & Ofodile, O. C. (2024). Reviewing the role of big data analytics in financial fraud detection. Finance & Accounting Research Journal, 6(3), 384-394.https://fepbl.com/index.php/farj/article/view/899

[9] Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931-952. https://fepbl.com/index.php/farj/article/view/1213

[10] Ellahi, E. (2024). Fraud Detection and Prevention in Finance: Leveraging Artificial Intelligence and Big Data. Dandao Xuebao/Journal of Ballistics, 36(1), 54-62. https://ballisticsjournal.com/index.php/journal/article/view/141

[11] Chowdhury RH, Reza J, Akash TR. EMERGING TRENDS IN FINANCIAL SECURITY RESEARCH: INNOVATIONS CHALLENGES, AND FUTURE DIRECTIONS. Global Mainstream Journal of Innovation, Engineering & Emerging Technology. 2024;3(04):31-41

[12] https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset

[13] Akash TR, Reza J, Alam MA. Evaluating financial risk management in corporation financial security systems. World Journal of Advanced Research and Reviews. 2024;23(1):2203-13