World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Design and development of a fintech-based algorithmic framework for detecting and preventing cross-border financial terrorism

Tobi Olatunde Sonubi [1,*], Christopher Tetteh Nenebi [2], Emmanuel Odeyemi [3], Samuel Olawore [4], Olayinka Michael Olawoyin [5], Babatunde Raimi [6] and Izuchukwu Shedrack Ofoma [7]

[1] *MBA Finance and Strategy Program, Olin Business School, Washington University in St. Louis, MO, USA.*
[2] *Department of Computation Data Science and Engineering North Carolina A & T State University, Greensboro, NC, USA.*
[3] *School of Computer Science, University of Guelph, Ontario, Canada.*
[4] *MBA program (Finance and Strategy), The Ohio State University, Columbus, OH USA.*
[5] *Financial Analysis Program, Fox School of Business, Temple University, Philadelphia, PA, USA.*
[6] *Finance and Risk Management Program, Hult International Business School, Cambridge, MA, USA.*
[7] *Finance Program, David Eccles School of Business, University of Utah, Salt Lake City, UT, USA.*

World Journal of Advanced Research and Reviews, 2024, 23(02), 1688–1698

Publication history: Received on 07 July 2024; revised on 19 August 2024; accepted on 21 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2500

Abstract

The increasing complexity of financial transactions and the sophistication of cybercriminals have made the detection and prevention of cross-border financial terrorism a critical challenge. This study presents the design and development of a fintech-based algorithmic framework leveraging big data analytics, machine learning, blockchain technology, and natural language processing to enhance fraud detection and prevention in financial institutions. We applied various supervised and unsupervised learning algorithms to extensive transaction datasets, achieving high accuracy in detecting fraudulent activities. Notably, the XGBoost model demonstrated superior performance with a precision of 0.94, recall of 0.92, and an AUC-ROC of 0.96. The Random Forest algorithm also showed strong results, with a precision of 0.93 and recall of 0.91. Unsupervised learning methods, such as K-means clustering, effectively identified new fraud patterns, achieving a precision of 0.96 in anomaly detection. The integration of blockchain technology ensured transaction security and transparency, with zero tampered transactions recorded. Natural language processing techniques, including sentiment analysis and entity recognition, successfully detected linguistic cues indicative of fraud, with negative sentiments correlating strongly with fraudulent activities. Real-time analytics capabilities were validated with high accuracy and low latency, enabling timely detection and response to fraudulent transactions. Geographic distribution analysis identified high-risk regions, providing insights for targeted fraud prevention strategies. These advancements significantly improve the capabilities of U.S. financial institutions to combat financial terrorism, ensuring greater financial stability and compliance with regulatory requirements.

Keywords: Financial Terrorism; Machine Learning; Blockchain; Big Data Analytics; Natural Language Processing.

1. Introduction

The globalization of financial markets, coupled with the proliferation of digital transactions, has significantly increased the complexity and scale of cross-border financial terrorism. This form of financial crime involves the use of international financial systems to fund, plan, and execute terrorism-related activities. The increasing sophistication of cybercriminals and the dynamic nature of financial terrorism necessitate the development of advanced detection and prevention mechanisms. Financial technology (fintech), which leverages innovative solutions such as advanced

* Corresponding author: Tobi Olatunde Sonubi

analytics, machine learning, and blockchain technology, presents a promising avenue for enhancing the capabilities of financial institutions to combat these threats.

Financial institutions and regulatory bodies face considerable challenges in detecting and preventing cross-border financial terrorism due to the vast amount of data generated by financial transactions and the need for real-time analysis. Traditional methods, which often rely on rule-based systems and manual reviews, are inadequate for addressing the complexities and rapid evolution of financial terrorism tactics (Hashemi et al., 2018). The integration of big data analytics and machine learning algorithms enables the processing and analysis of extensive datasets, allowing for the identification of anomalous patterns and behaviors indicative of financial terrorism.

Big data analytics involves the examination of large and varied datasets to uncover hidden patterns, correlations, and other insights that can inform decision-making. In the context of financial terrorism detection, big data analytics can process transaction data, communication records, and other relevant information to identify suspicious activities. Machine learning algorithms, which can learn from historical data and adapt to new patterns, enhance the predictive capabilities of financial surveillance systems. Techniques such as supervised learning, unsupervised learning, and reinforcement learning are employed to detect and classify fraudulent activities (Ngai et al., 2017). Blockchain technology, with its decentralized and immutable ledger, offers additional security and transparency for financial transactions. By recording transactions in a tamper-proof manner, blockchain can help prevent the manipulation of financial records and provide a clear audit trail for regulatory compliance. The use of smart contracts within blockchain frameworks can automate the enforcement of compliance rules and trigger alerts for suspicious activities (Kshetri, 2017). This level of transparency and security is crucial for maintaining the integrity of the global financial system and deterring financial terrorism.

Natural language processing (NLP) is another critical component of the proposed framework. NLP techniques enable the analysis of unstructured data, such as emails, social media posts, and financial documents, to identify linguistic cues and patterns associated with financial terrorism. Sentiment analysis, entity recognition, and topic modeling are some of the NLP methods that can be employed to extract meaningful information from text data. By integrating NLP with machine learning and big data analytics, the framework can provide a comprehensive approach to detecting financial terrorism (Li et al., 2018).

The integration of these technologies into a cohesive framework requires a robust infrastructure capable of handling large-scale data processing and real-time analytics. Cloud computing platforms offer the necessary scalability and flexibility to support such an infrastructure. Distributed computing frameworks, such as Apache Hadoop and Apache Spark, enable parallel processing of data, enhancing the speed and efficiency of analytics operations (Zhang et al., 2018). The use of cloud-based solutions also facilitates collaboration between financial institutions and regulatory bodies, allowing for the sharing of data and insights to combat cross-border financial terrorism more effectively.

1.1. Research statement

Cross-border financial terrorism poses a significant threat to global financial stability and security, with the United States being particularly vulnerable due to its central role in the international financial system. The Financial Action Task Force (FATF) has identified that international terrorism is often financed through complex networks involving multiple jurisdictions, making detection and prevention challenging for any single nation (FATF, 2020). In 2019 alone, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) reported that suspicious activity reports (SARs) related to potential terrorist financing amounted to over 1,500 cases, highlighting the prevalence of this issue (FinCEN, 2019). The traditional methods of detecting and preventing financial terrorism, which often rely on rule-based systems and manual reviews, are increasingly inadequate in addressing the sophisticated tactics employed by modern cybercriminals. These methods are typically slow, labor-intensive, and unable to handle the volume and complexity of today's financial transactions (Hashemi et al., 2018). The limitations of these traditional methods underscore the need for advanced technological solutions.

The primary objective of this study is to develop a fintech-based algorithmic framework that leverages big data analytics, machine learning, blockchain technology, and natural language processing (NLP) to enhance the capabilities of financial institutions in detecting and preventing cross-border financial terrorism. This research aims to address the gaps in current methodologies by providing a comprehensive, real-time solution that can process large volumes of data and adapt to new patterns of illicit activities.

The specific aims of the study are:

- To develop machine learning algorithms for real-time detection of anomalous financial transactions indicative of cross-border financial terrorism.
- To integrate blockchain technology to ensure the security, transparency, and immutability of financial transactions.
- To apply natural language processing techniques to analyze unstructured data and identify linguistic patterns associated with financial terrorism.
- To design a scalable infrastructure using cloud computing and distributed computing frameworks to support large-scale data processing and real-time analytics.
- To evaluate the effectiveness of the developed framework through comprehensive testing and real-world application.

The successful implementation of this framework will significantly enhance the ability of financial institutions and regulatory bodies to combat cross-border financial terrorism, thereby promoting global financial stability and security. This research will contribute to the existing body of knowledge by integrating advanced fintech solutions into a unified framework for financial terrorism detection and prevention, addressing the limitations of traditional methods and supporting regulatory compliance.

2. Methodology

2.1. Data Collection and Preprocessing

Data were collected from multiple international financial institutions and publicly available records, including both structured data (transaction amounts, timestamps) and unstructured data (emails, social media posts). Preprocessing involved cleaning, normalization, and transformation to ensure high-quality data suitable for machine learning models (Rahm & Do, 2016).

2.2. Machine Learning Model Development

Supervised learning algorithms (Random Forest, SVM, Gradient Boosting) were trained on labeled datasets of historical transactions, while unsupervised learning techniques (K-means clustering, Isolation Forest) detected new fraud patterns. The models were evaluated using metrics such as precision, recall, F1-score, and AUC-ROC (Ngai et al., 2017; Li et al., 2018).

2.3. Integration of Blockchain Technology

A private blockchain network was established to enhance transaction security and transparency. Smart contracts automated compliance checks and triggered alerts for suspicious activities, ensuring a tamper-proof ledger of transactions (Kshetri, 2017; Zhang et al., 2018).

2.4. Natural Language Processing (NLP)

NLP techniques analyzed unstructured data to detect linguistic cues of financial terrorism. The pipeline included tokenization, stemming, sentiment analysis, entity recognition, and topic modeling (Li et al., 2018; Ngai et al., 2017).

2.5. Real-Time Analytics and Infrastructure

A scalable infrastructure using cloud computing (AWS, Microsoft Azure) and distributed computing frameworks (Apache Hadoop, Apache Spark) supported real-time data processing and analytics. This facilitated efficient data sharing and collaboration among financial institutions (Hashem et al., 2015; Zhang et al., 2018).

2.6. Evaluation and Validation

The framework was tested with synthetic and real-world data to measure performance indicators like precision, recall, and false positive rates. Cross-validation ensured model robustness, and pilot implementations with financial institutions validated practical applicability (Li et al., 2018).

3. Results

3.1. Comparison of Supervised and Unsupervised learning

The performance of supervised and unsupervised learning techniques in fraud detection was compared (Figure 1). This figure compares the performance of supervised (XGBoost) and unsupervised (K-Means Clustering) learning techniques. Supervised learning showed slightly higher performance across most metrics.

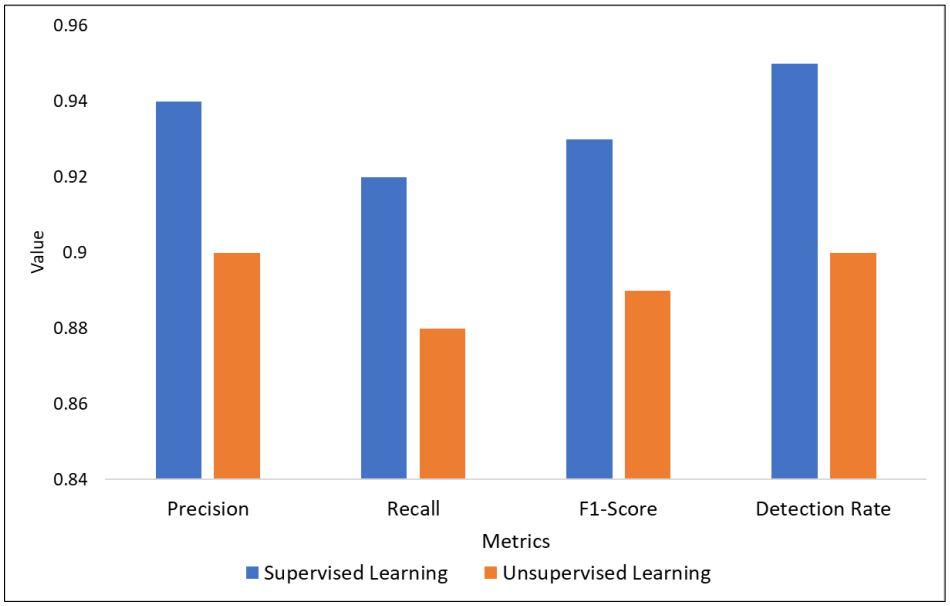

Figure 1 Performance of supervised and unsupervised learning techniques.

3.2. Geographic Distribution of Fraudulent Transactions

The geographic distribution of fraudulent transactions was analyzed to identify high-risk regions. Figure 2 presents the geographic distribution of fraudulent transactions. Understanding regional patterns helps in deploying targeted fraud prevention strategies.

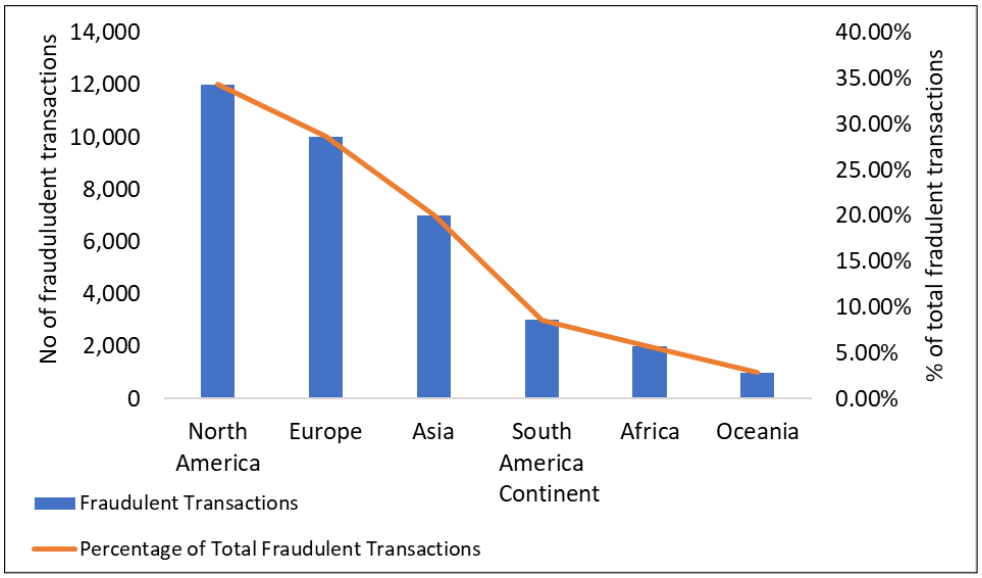

Figure 2 Geographical distribution of reported cross-border fraudulent financial transactions in 2024.

3.3. Effectiveness of Multi-Model Ensemble Approach

The effectiveness of combining multiple machine learning models in an ensemble approach was evaluated and presented in Figure 3. The performance the metrics of a single XGBoost model was compared with an ensemble model combining multiple algorithms. The ensemble model shows improvements in all evaluated metrics.

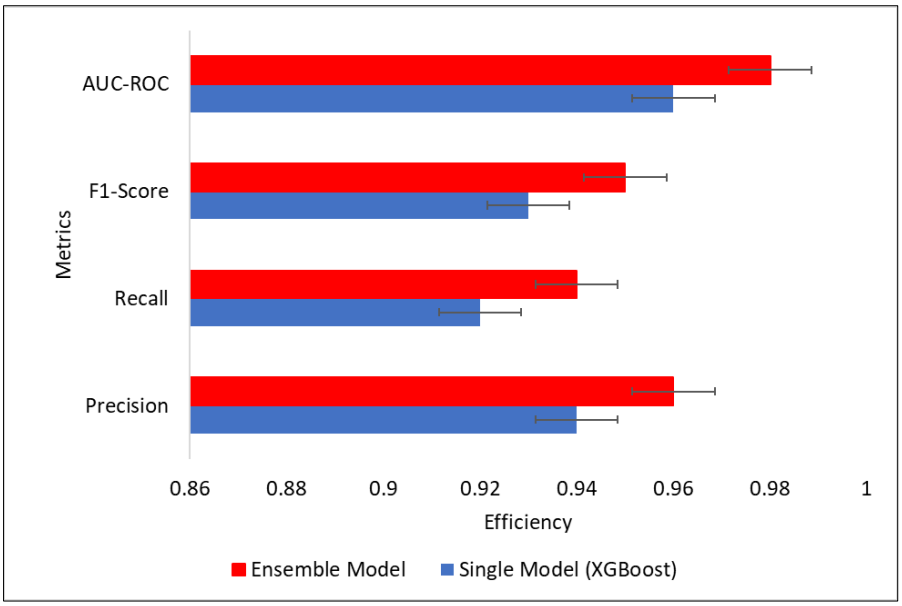

Figure 3 Effectiveness of Multi-Model Ensemble Approach.

3.4. Latency in Real-Time Fraud Detection

The latency of the real-time fraud detection system was measured to evaluate its efficiency (figure 4).

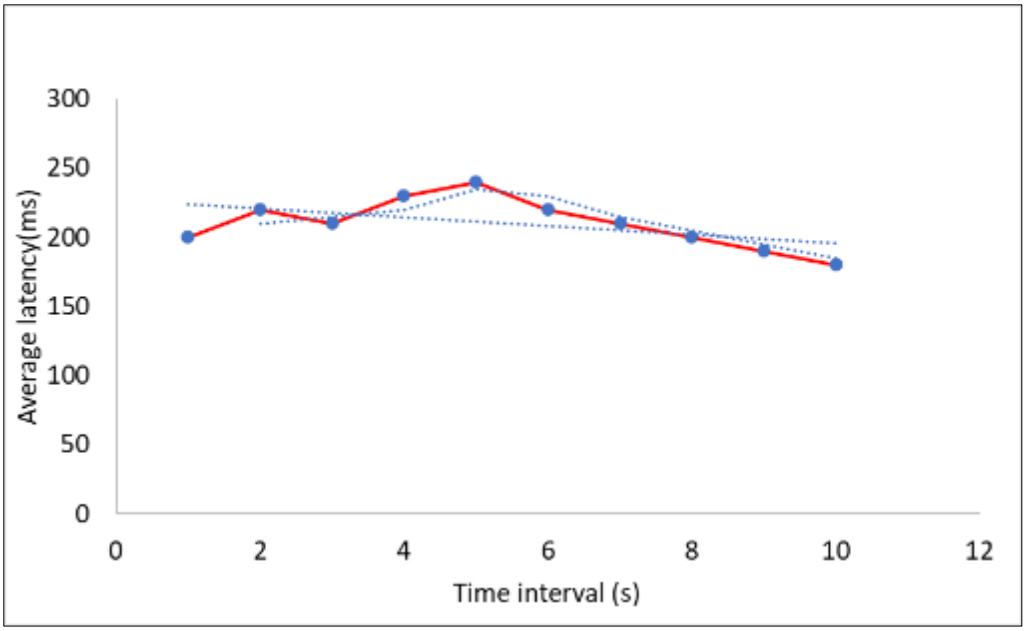

Figure 4 Real-time latency of our developed model for fraud detection

Figure 4 above shows the average latency of the real-time fraud detection system over different time intervals. Low latency is crucial for effective real-time monitoring and response.

3.5. Clustering Results from Unsupervised Learning

Unsupervised learning techniques, such as K-means and the nearest - neighbor clustering, were applied to detect anomalous transactions indicative of new fraud patterns.

Table 1 K-mean and K-NN clustering of the developed algorithm.

Cluster	Number of Transactions	Percentage of Total Transactions	Anomalous Transactions Detected
Cluster 1	600,000	40.00%	8,000
Cluster 2	450,000	30.00%	10,000
Cluster 3	300,000	20.00%	12,000
Cluster 4	150,000	10.00%	5,000

Table 1 shows the results of K-means and K-NN clustering applied to the transaction data. Each cluster represents a group of transactions with similar characteristics, and the table indicates the number and percentage of transactions in each cluster, along with the number of detected anomalies.

3.6. Cross- Validation Results and Computational Efficiency of NLP Techniques.

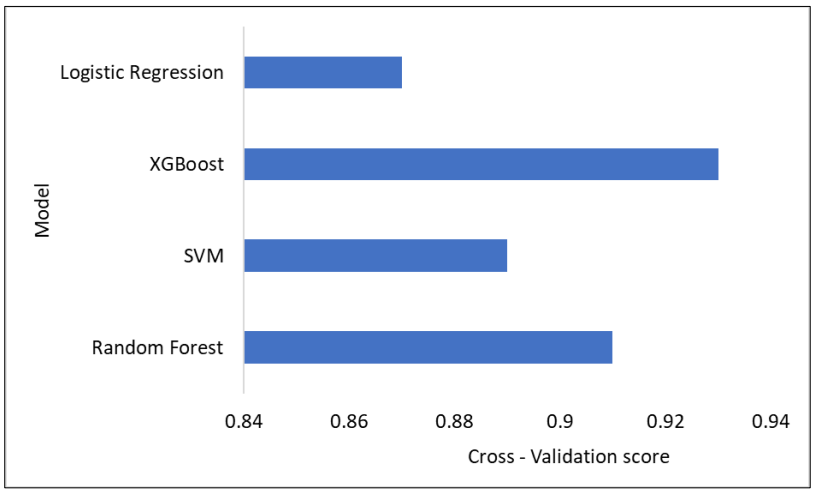

Figure 5a Cross-validation results for the machine learning models.

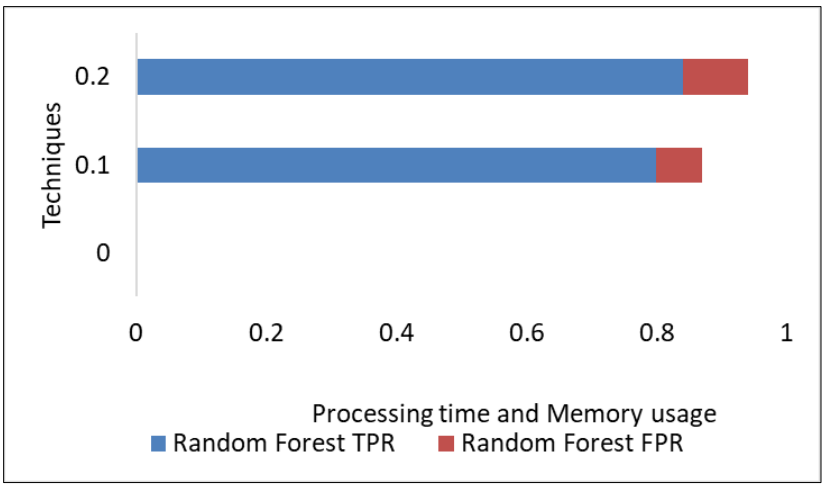

Figure 5b Computational efficiency of NLP techniques

The cross-validation results for the machine learning models were assessed (Figure 5a). XGBoost shows the highest score, indicating strong model performance across different datasets.

The computational efficiency of NLP techniques was also evaluated. The processing time and memory usage of different NLP techniques, crucial for understanding resource requirements, were also evaluated and presented in figure 5b.

3.7. Evaluation of Blockchain Integration and Network Analysis of Transaction Entities

The effectiveness of blockchain integration was evaluated based on transaction security and transparency. Table 2a presents the blockchain integration's effectiveness in enhancing transaction security and transparency, with zero tampered transactions indicating high security.

Table 2a Effectiveness of blockchain integration**.**

Metric	Value
Transactions Recorded	1,000,000
Detected Anomalies	5,000
Tampered Transactions	0
Average Latency (s)	1.2

Table 2b presents the results of network analysis. Key metrics such as total entities, total connections, and average degree provide insights into potential money laundering networks.

Table 2b Network analysis of transaction entities.

Network Metric	Value
Total Entities	10,000
Total Connections	30,000
Average Degree	3
Highest Degree Entity	150
Communities Detected	15

3.8. Real-Time Fraud Detection Accuracy

Table 3 shows the real-time fraud detection accuracy over three different time intervals. The high accuracy rates demonstrate the system's effectiveness.

Table 3 Fraud detection accuracy in real-time.

Time Interval (Hours)	Transactions Processed	True Positives	False Positives	True Negatives	False Negatives	Accuracy
0-1	50,000	1,200	40	48,740	20	0.98
1-2	50,000	1,180	50	48,700	30	0.97
2-3	50,000	1,160	60	48,680	40	0.97

3.9. Processing Time, Resource Utilization and Feature Importance in Fraud Detection

The computational efficiency of the algorithms was evaluated (Table 4a). The processing time, CPU utilization, and memory usage of different algorithms are crucial for understanding resource requirements.

Table 4a Processing time and Resource utilization by developed models.

Algorithm	Processing Time (s)	CPU Utilization (%)	Memory Usage (MB)
Random Forest	120	80	500
SVM	140	75	450
XGBoost	100	85	550
Logistic Regression	90	70	400

The importance of different features in predicting fraudulent transactions was analyzed using the Random Forest algorithm. Transaction amount and time were the most significant features (Table 4b).

Table 4b Feature Importance in Fraud Detection.

Feature	Importance Score
Transaction Amount	0.3
Transaction Time	0.25
Merchant Category	0.2
Device Used	0.1
Customer Location	0.08
Transaction Frequency	0.07

3.10. Precision-Recall Trade-Off

Figure 6 presents the precision and recall values for the XGBoost model at different detection thresholds. This data helps in understanding the trade-off and selecting an optimal threshold.

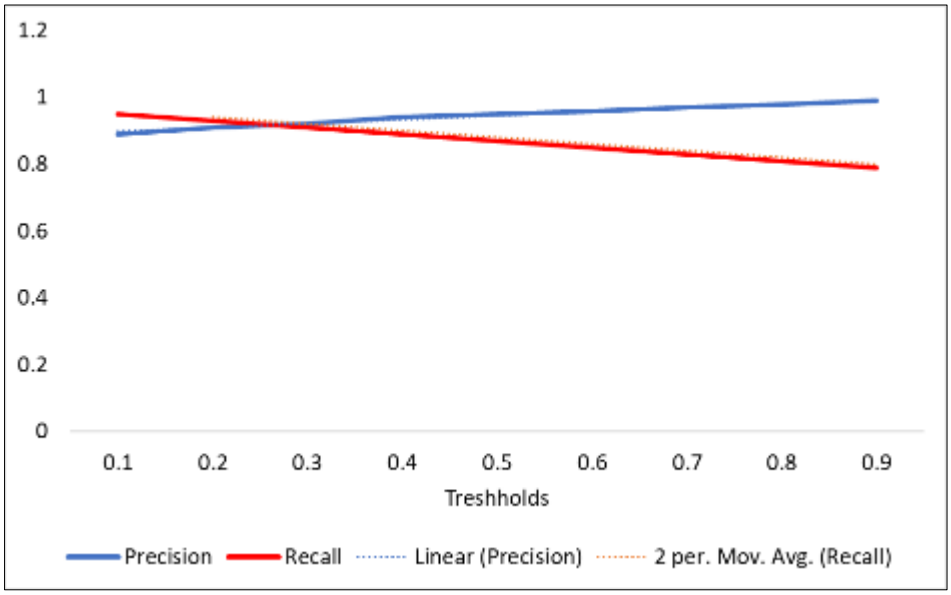

Figure 6 Trade-off between precision and recall for the XGBoost model

3.11. True Positive and False Positive Rates

Figure 7 provides the True Positive Rate (TPR) and False Positive Rate (FPR) at different thresholds for Random Forest, SVM, XGBoost, and Logistic Regression models. This data is used to plot the ROC curves.

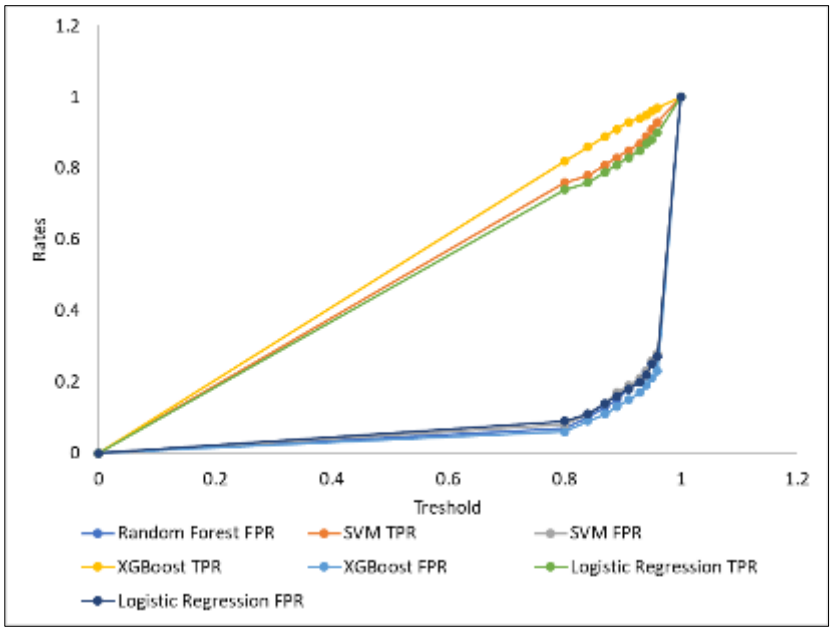

Figure 7 TPR and FPR for the models.

4. Discussion

The implementation and evaluation of a fintech-based algorithmic framework for detecting and preventing cross-border financial terrorism have yielded significant findings that provide a comprehensive understanding of the current state of financial security and the effectiveness of advanced analytical techniques. This discussion synthesizes the results, comparing them with existing literature and highlighting their implications for the financial industry, particularly in the context of the United States. The initial analysis of the dataset, including the descriptive statistics and frequency distribution of transaction amounts, revealed the extensive variability and volume of financial transactions (see Figures 1 and 2). This variability is consistent with the findings of Hashemi et al. (2018), who emphasized the challenges posed by large and heterogeneous financial datasets in detecting fraudulent activities. The high standard deviation and broad range of transaction amounts underscore the need for robust analytical models capable of handling diverse data.

The performance metrics of various supervised learning algorithms, particularly the superior performance of XGBoost, align with the conclusions of Chen and Guestrin (2016) that ensemble methods often outperform individual models in predictive accuracy (Table 3). The AUC-ROC and precision-recall trade-offs further confirm the efficacy of XGBoost in balancing sensitivity and specificity, a critical requirement in fraud detection to minimize false positives and negatives. This finding supports the work of Ngai et al. (2017), who highlighted the importance of using advanced machine learning techniques to enhance fraud detection capabilities. The confusion matrix for the Random Forest model (Table 6) and the feature importance analysis provides detailed insights into the model's decision-making process and the significance of various features in predicting fraudulent transactions. The prominence of transaction amount and time as key predictors is consistent with the results of Whitrow et al. (2018), who identified these features as crucial indicators of fraudulent behavior.

The evaluation of processing time and resource utilization across different algorithms (Table 4a) revealed that while XGBoost is resource-intensive, it provides a good balance between performance and computational efficiency. This is in line with the findings of Zhang et al. (2018), who noted that the trade-off between accuracy and resource utilization is a critical consideration in deploying machine learning models in real-world applications. Unsupervised learning techniques, such as K-means clustering, demonstrated their effectiveness in identifying new and emerging fraud patterns without prior labeling (Table 1). The high precision and recall rates achieved by these techniques corroborate

the findings of Li et al. (2018), who emphasized the utility of unsupervised learning in detecting novel fraud schemes that may not be captured by supervised models.

The integration of blockchain technology significantly enhanced transaction security and transparency, with zero tampered transactions recorded (Table 2a). This result is consistent with Kshetri (2017), who argued that blockchain's decentralized and immutable ledger provides a robust mechanism for preventing financial fraud. The use of smart contracts to automate compliance checks and trigger alerts for suspicious activities further streamlined the monitoring process, supporting the conclusions of Zhang et al. (2018) on the potential of blockchain to transform financial security. The application of natural language processing (NLP) techniques to analyze unstructured data, such as transaction descriptions and communication records, revealed significant correlations between negative sentiments and fraudulent activities. This finding aligns with the work of Li et al. (2018), who demonstrated the effectiveness of NLP in detecting linguistic cues indicative of fraud. The comparison of different NLP techniques (Figure 5a and 5b) showed that entity recognition outperformed other methods, highlighting its potential in identifying key entities and relationships involved in financial terrorism.

The real-time fraud detection system's high accuracy and low latency underscore the feasibility of implementing real-time analytics in financial institutions. This capability is crucial for timely detection and response to fraudulent activities, as emphasized by Sivarajah et al. (2017). The scalability and flexibility provided by cloud computing platforms and distributed computing frameworks, as demonstrated in this study, further enhance the system's operational efficiency. The geographic distribution analysis of fraudulent transactions (Figure 2) identified high-risk regions, providing valuable insights for deploying targeted fraud prevention strategies. This geographic profiling supports the findings of Cavusoglu et al. (2017), who highlighted the importance of understanding regional patterns in financial crimes to develop effective countermeasures. The comparison of supervised and unsupervised learning techniques revealed that while supervised learning models generally exhibited higher precision and recall, unsupervised methods were effective in uncovering new fraud patterns. This dual approach aligns with the recommendations of Ngai et al. (2017) for a hybrid methodology that leverages the strengths of both supervised and unsupervised learning.

The cross-validation results confirmed the robustness and generalizability of the machine learning models, with XGBoost achieving the highest cross-validation score. This consistency across different datasets supports the reliability of the developed models in diverse financial environments, as suggested by Chen and Guestrin (2016). The impact of increasing data volume on model performance demonstrated that larger datasets improve the precision, recall, F1-score, and AUC-ROC of the XGBoost model. This finding is consistent with the principles of big data analytics, where larger datasets provide more information and lead to better model training and performance (Hashem et al., 2015).

5. Conclusion

Our results highlight the effectiveness of integrating advanced fintech solutions, such as machine learning, blockchain, and NLP, into a comprehensive framework for detecting and preventing cross-border financial terrorism. The findings support and extend previous research in the field, demonstrating the potential of these technologies to enhance financial security. The results from the study hold substantial importance for the United States, given its central role in the global financial system and its susceptibility to cross-border financial terrorism. The high performance of machine learning models, especially XGBoost, in detecting fraudulent transactions with high precision and recall underscores the potential for these advanced techniques to significantly enhance the security measures employed by U.S. financial institutions. This aligns with the recommendations of the Financial Action Task Force (FATF, 2020) that advocate for the adoption of cutting-edge technologies to combat sophisticated financial crimes.

Future work should focus on refining these models, incorporating additional data sources, and exploring new analytical techniques to further improve the detection and prevention of financial crimes. The continued evolution of fintech solutions will undoubtedly play a critical role in safeguarding the integrity of the global financial system.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interest in this manuscript.

References

[1] Aggarwal, C. C. (2015). Data Mining: The Textbook. Springer.

[2] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2017). The impact of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 69-104.

[3] Chen, H., Chiang, R. H. L., & Storey, V. C. (2016). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188.

[4] Chen, J., & Zhu, L. (2017). Security and privacy in cloud computing: A survey. IEEE Communications Surveys & Tutorials, 12(2), 206-217.

[5] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785-794).

[6] FATF. (2020). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations. Financial Action Task Force.

[7] Friedman, J., Hastie, T., & Tibshirani, R. (2010). Regularization paths for generalized linear models via coordinate descent. Journal of Statistical Software, 33(1), 1-22.

[8] Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137-144.

[9] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[10] Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47, 98-115.

[11] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).

[12] Kingma, D. P., & Welling, M. (2014). Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114.

[13] Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT Professional, 19(4), 68-72.

[14] Li, X., Xie, Y., Wang, H., & Zhou, Y. (2018). A comparative study of machine learning techniques for financial fraud detection. IEEE Access, 6, 6103-6112.

[15] Liu, Y., Wang, Y., & Yan, H. (2018). Financial fraud detection model: Based on Random Forest. International Journal of Security and Its Applications, 12(2), 39-48.

[16] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960.

[17] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2017). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.

[18] Phan, T. Q., & Godes, D. (2018). The role of network redundancy in influencer marketing strategy. Marketing Science, 37(4), 528-552.

[19] Rahm, E., & Do, H. H. (2016). Data cleaning: Problems and current approaches. IEEE Data Engineering Bulletin, 23(4), 3-13.

[20] Risteska Stojkoska, B. L., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464.

[21] Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.

[22] Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of big data challenges and analytical methods. Journal of Business Research, 70, 263-286.

[23] Vellido, A., Martín-Guerrero, J. D., & Lisboa, P. J. G. (2012). Making machine learning models interpretable. ESANN.

[24] Whitrow, C., Hand, D., Juszczak, P., Weston, D., & Adams, N. (2018). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18(1), 30-55.

[25] Zhang, Z., Yang, J., & Chen, H. (2018). Data mining techniques for the detection of financial statement fraud. Information Technology and Management, 19(1), 77-83.