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

Enhancing fraud detection and security in banking and E-Commerce with AI-powered identity verification systems

Md Abdul Alim [1,*], Md Reduanur Rahman [2], Md Habibul Arif [3] and Md Shakhawat Hossen [4]

[1] *Bachelor of Business Administration (BBA in Finance), Northern University, Bangladesh.*
[2] *Bachelor of Arts with Honours in Marketing Management, London School of Management Education, Ilford, England.*
[3] *Bachelor of Science in Computer Science and Engineering, Dhaka International University, Bangladesh.*
[4] *Bachelor of Arts with Honours in English, National University, Bangladesh.*

World Journal of Advanced Research and Reviews, 2020, 06(03), 313-322

Publication history: Received on 14 May 2020; revised on 20 June 2020; accepted on 28 June 2020

Article DOI: https://doi.org/10.30574/wjarr.2020.6.3.0205

Abstract

The ever-increasing digital banking and e-commerce has increased the financial frauds done using client-side cultural IP protocol. These systems find it difficult to catch up to the increasing transaction complexity. 'Fraud detection is vital for banks and e-commerce systems to prevent losses and protect users, so it's important for the computer systems to be sound in the digital age. In this paper AI based fraud detection system using machine learning algorithms such as Logistic Regression, Random Forest, Gradient Boosting (GBM), XGBoost and Light GBM have been suggested. To handle the class imbalance, we use SMOTE (Synthetic Minority Over-sampling Technique) for balancing the dataset and enhancing model performance. The accuracy, precision, recall, and F1-score were computed to evaluate the models. Results indicated that Gradient Boosting and LightGBM obtained the best performances when SMOTE was used to augment fraud detection. Our finding proved the success of AI and ML as fraud-detecting technique. SMOTE, being a method to overcome class-imbalance is incorporated but more fine-tuning should be done to combat changing fraudulent strategies. Dynamic model updating and feature engineering are needed to ensure the robustness of fraud detection systems in digital financial services applications.

Keywords: AI-driven fraud detection; Banking transactions; Identity verification; E-commerce security; SMOTE; Fraud prevention; Real-time transaction

1. Introduction

The quick digitalization of financial transactions in banks and e-commerce faces opportunities and threats. Benefiting from the added sense of access and ease, these industries are also now more vulnerable to fraudulent attacks. For example, in 2019, financial losses worldwide due to fraud were projected to be over $28 billion, and a large percentage of that amount came from e-commerce scams Internet Crime Complaint Center [1]. Conventional fraud detection systems based on manual inspection and rule-based models face challenges to be able to coping with the increasing complexity and volume of transactions. Consequently, the financial institutions have resorted to AI and ML so that these challenges can be conquered efficiently, whereby the fraud detection process may be improved—rise of AI in next-gen fraud detection. In today's digital finance world, traditional approaches do not cut it. It makes it possible for banks to automate fraud detection and augment the ability to detect fraudulent activities with higher rotation and in real-time. AI technologies like machine learning and deep learning make it possible to analyze large quantities of transaction data, making it easier to detect anomalies and predict fraudulent activities. This dramatically lowers false positives and improves the overall operational efficiency. AI-powered applications were found to be able to lower exposure-related costs by as much as 25% last year, making the advanced technology particularly critical in fraud detection systems, Internet Crime Complaint Center [1]. The role of AI in fraud prevention is widespread, not only for its adaptability to

* Corresponding author: Md Abdul Alim

new types of fraud. Legacy systems are not very good at learning to detect new types of fraud, but AI models can be updated with each new fraudulent scheme, allowing them to stay ahead in order to combat future threats. One such example of the use of AI comes from studies conducted in 2019, which found that AI-enabled fraud detection systems can cut the time taken to detect fraud by more than half, enabling firms to catch and take action against fraudulent activity on the internet as it is taking place (Internet Crime Complaint Center). Furthermore, using AI with identity verification and authentication technology improves security for digital transactions, which creates user confidence to propel the growth of digital financial services. We are all aware that over the last year, there have been entire waves in computing and security. Multiple algorithms are in place when it comes to AI fraud detection systems, and each one plays a vital role in detecting fraudulent transactions. CONCLUSION: Traditional machine learning models like Random Forest, XGBoost, and Gradient Boosting are standard techniques to analyze transactional data by identifying patterns and anomalies that lead to fraud. They are ideal for imbalanced datasets, which is typically the case in fraud detection. Deep learning models, such as NN (neural networks), are also employed to find out the complex patterns that are not easily discovered by conventional methods. Unstructured data, including user behavior and communication patterns, is analyzed using anomaly detection and natural language processing (NLP), enhancing the accuracy of detected fraud Internet Crime Complaint Center. In this study, we introduce a novel AI-enabled fraud-detecting framework for banking and e-commerce transactions. Our model seamlessly integrates cutting-edge machine learning algorithms and AI-based KYC/identity verification systems to deliver a scalable, proven solution to anti-fraud. The platform centers on the real-time detection of fraud by processing data from various sources for better visibility into potentially fraudulent occurrences. Our solution incorporates both fraud detection and identity verification, allowing only real users to perform transactions with an extra layer of trust. Such an amalgamation can make financial ecosystems more secure, systemically sound, and trustworthy.

This paper discusses several topic areas and provides a brief literature review in section two. Section III describes the procedures employed, and Section IV gives the experimental results. In Section V, we discuss the performance of our proposed model. Finally, Section VI provides a more comprehensive review of these mechanisms.

2. Literature review

Prosper el at [2] This paper focuses on the issues of AI Realisation in Omni Channel Sales from the scale, secure aspect and from the performance aspect. It studies the use of microservices, containerization and cloud platforms for AI frameworks in emerging hyper-scale transactions, as well as counter-challenging measures to protect these consumables solutions enabled with AI capabilities. The report includes best practices and advanced recommendations like generative AI, federated learning to help increase customer engagement and business responsiveness in digital sales strategies.

Nelson el at [3] This paper explores how AI and ML techniques can be used in financial risk management with emphasis on fraud detection using big data analytics methodologies such as Node2Vec. The Node2Vec method can capture the structural relation between nodes in financial networks, leading to enhanced accuracy of fraud detection when applied in a deep neural network (DNN). Empirical evaluation results show that the Node2Vec-DNN model has better performance than traditional models with F1-scores between 67.1% and 73.4%. The research also demonstrates the use case of graph-based deep learning techniques to improve financial fraud detection and risk management.

Mbah el at [4] This Article discusses the Bank Verification Number (BVN) in Nigeria and its distinctive features towards enhancing financial security and identity consolidation. It acknowledges the weaknesses in existing laws with respect to data privacy and protection, the apprehension of lacunae in regulation and the absence of a robust data protection law. By comparing Nigeria's strategy with the European Union GDPR, suggestions to improve data privacy policy and cybersecurity are given in this paper. It is important to further consolidate this legislation for consumer trust and safety in the Nigerian digital banking space, especially with recent cybersecurity threats.

Lau el at [5] Article details the future of financial services and explains how AI and Machine Learning can empower contextually aware personalised interaction to deliver maximised customer value. Using customer data, the research demonstrates how financial services providers can leverage trust and empathy to develop closer brand relationships with their customers. It highlights the role that AI can play in a more inclusive financial system, whose echoes may last for generations in health and wealth. The paper calls for algorithmic rethinking, including on financial safety overall and social welfare generation in the emerging service platforms.

Kumar el at [6] This paper explores the way PFM systems, based upon AI technologies, use different methods such as machine learning, natural language processing and predictive analytics to exploit financial planning. It delivers real-time recommendations and detects anomalies based on data from various financial sources. The study benchmarks PFM

tools based on modern AI against legacy solutions, with a specific focus on their impact on user behaviour. Also at play were concerns around privacy, model transparency and future improvements to build more customized and safer versions.

Adenekan el at [7] This post explores the industry movements and shifts shaping the future of FinTech: decentralized finance (DeFi), open banking, and embedded finance. It is covering how transformative technologies like AI, blockchain and machine learning drive new opportunities in finance. Finally, the study's attention has been centred on the increase of consumer views and attitudes after the surge of FinTech and its implications for policy making. It concludes with a few words about what this might imply for FinTech firms and traditional institutions.

Prosper el. at [8] This article discusses what cloud-native AI architectures mean for omnichannel retail in terms of scalability, flexibility and real-time data processing. It speaks to how AI applications for hyper-personalised recommendations, predictive forecasting and automated decision-making are not new. However, there have been limitations regarding data syncing (like CRM systems), hot patches and security. It touches on generative AI and quantum AI for retail optimisation. It ends with tactical tips for smooth AI integration to drive positive CX and business continuity.

3. Material and methods

The objective of this research is to design and test an IFT system for banking and e-society type transactions. Several steps were taken during the process [9].

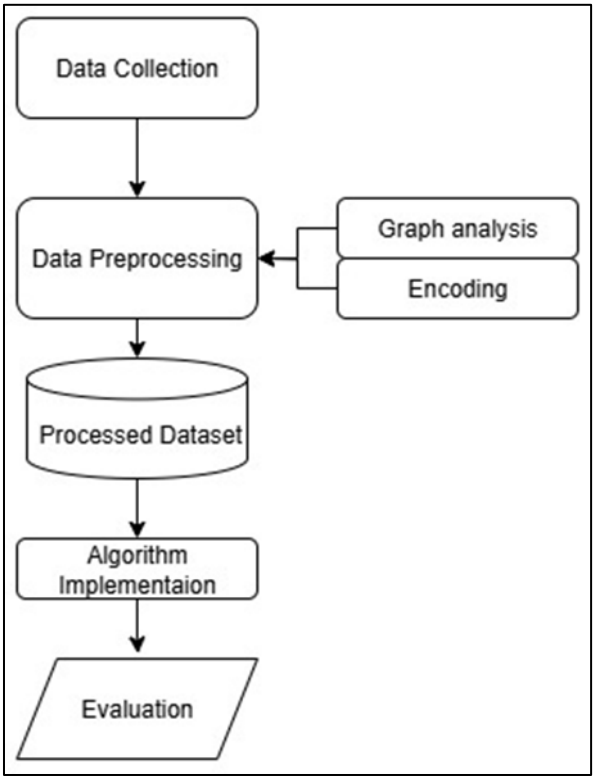

Figure 1 Methodology Diagram

3.1. Data collection

We were given a dataset that have transaction data including information such as transaction amount, user details and the transaction time stamps, however we do not know for each of these transactions if it was fraud or not [10].

3.2. Dataset pre-pressing and representation

We preprocessed the data, by way of handling missing values and normalizing numerical features, encoding categorical variables. We also dealt with the problem of class imbalance by means of the SMOTE technique, which creates synthetic fraud cases to help to train better our models [11]. Figure 2 "Distribution of Transaction Amounts" displays the

frequency distribution of transaction amounts at various values, as a hybrid of histogram and kernel density estimate (KDE) plot. The x-axis is transaction size 0 -10,000 and the y-axis plots number of transactions within each bin. With the histogram bars being even, it's indicating that transactions amounts are fairly evenly distributed throughout the range [12]. The KDE curve (superimposed on the histogram) is slightly peaked at lower transaction amounts, which corresponds to a higher proportion of the transactions being low-value. For a higher amount of transactions, the number of transactions that occur. The distribution indicates that transactions are fairly homogeneously distributed, but maybe an increased probability for small amounts of transactions.

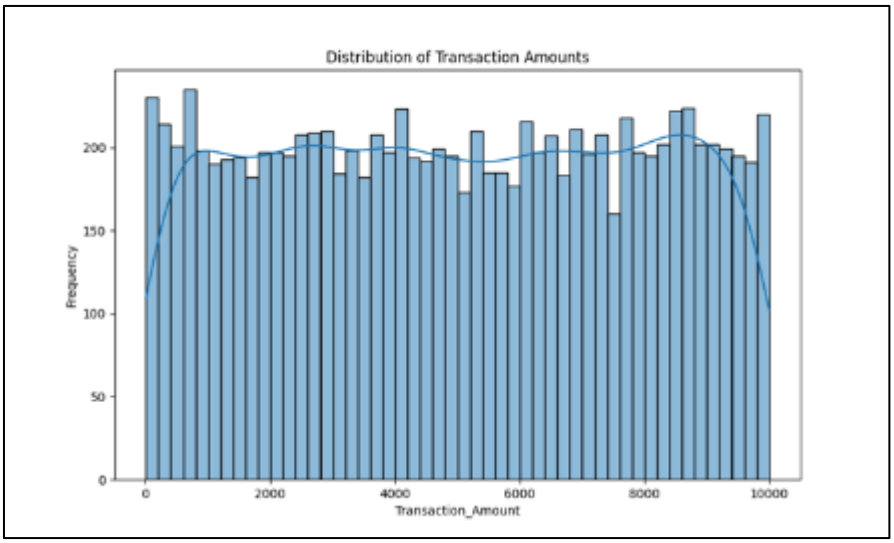

Figure 2 Distribution of Transaction Amounts

The boxplot "Transaction Amounts by Fraud vs. Non-Fraud" helps compare the transaction amounts in fraudulent vs non-fraudulent transactions shows as figure 3. Two categories of transactions were plotted against amount on the y-axis: '0' for non-fraud transactions, and '1' for fraud transactions. The distribution for non-fraud transactions follows the center around a transaction amount of about 4,000, with quite a symmetric spread and some outliers at the higher amount end (thus corresponding to most non-fraud transactions being for moderate amounts). Fraudulent transactions, on the other hand, also have a higher average around the same; however, have more variation in their amounts, including some extreme outliers, implying that they will be way more disproportionate [13][14]. In general, although some non-fraud and fraud transaction ranges overlap each other, the distribution of fraudulent transactions is broader than that for non-fraudulent ones, indicating a greater variation in the sizes of fraudulent activity.

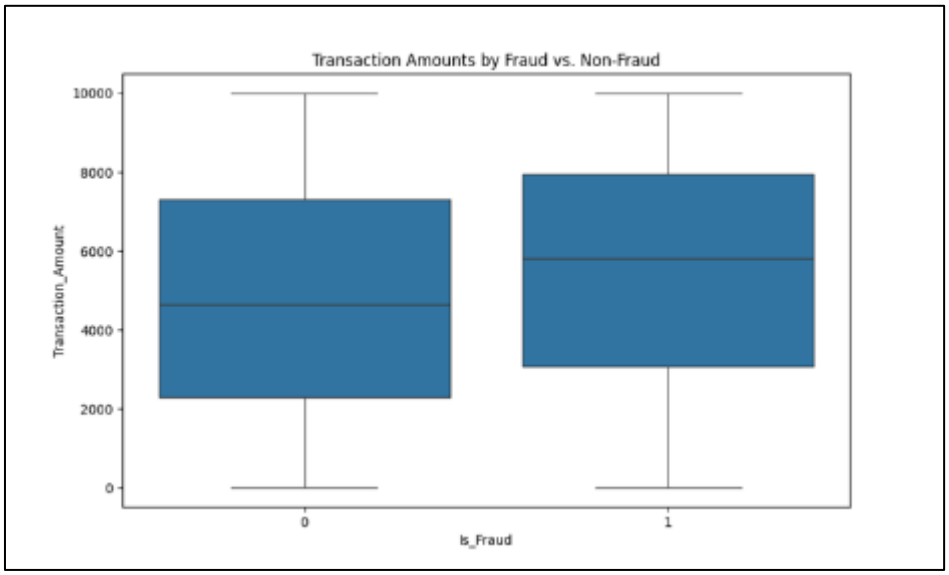

Figure 3 Transaction Amounts by Fraud vs. Non-Fraud

3.3. Model selection and algorithms

In this study, multiple machine learning algorithms such as Logistic Regression (LR), Random Forest (RF), Gradient Boosting Machine (GBM), XGBoost and LightGBM are selected for comparison [15]. We selected these models as they are capable of processing big data and have a strong classification power.

3.4. Evaluation

The one of the well-trained models performed on processed dataset were tested using accuracy, precision, recall and f1-score [16]. Cross-validation was also used to determine its robustness for model evaluation

4. Results and discussion

AI-based fraud detection systems are supported by a range of different algorithms, all to varying degrees, being instrumental in spotting fraudulent transactions. Familiar machine learning algorithms, Random Forest, XGBoost, Gradient Boosting, and LightGBM, are commonly used to mine transactional data, observing patterns and deviations that would point out a fraud being committed [17]. These classifiers work particularly well when outputting whether a transaction was legitimate or fraudulent by extracting features from the data.

Logistic Regression shown as table 1, had an accuracy of 0.68. It also yielded good results for class 0, with a precision of 0.81, a recall of 0.73, and F1-score of 0.77. Phenotype class 1 was less powerful precision: 0.45, a recall: 0.55, and an F1-score: 0.50. This resulted in a macro average F1-score of 0.63, suggesting balanced yet suboptimal performance. We also introduced the weighted average F1-score, which was 0.69 and exhibited an improvement when dealing with imbalanced classes [18]. This model has a difficult time detecting fraud (class 1) as compared to class 0.

Table 1 Accuracy table for Logistic Regression.

Label	Precision	Recall	F1-score	Support
0	0.81	0.73	0.77	1432
1	0.45	0.55	0.50	568
accuracy			0.68	2000
macro avg	0.63	0.64	0.63	2000
weighted avg	0.70	0.68	0.69	2000

The accuracy of Random Forest is shown as table 2, 0.6885. It performed well on class 0 with a precision of 0.78, a recall of 0.79, and an F1-score also found to be 0.78. However, for class 1, it performed poorly on precision (0.45), recall (0.42), and F1-score (0.44). The macro average F1-score was 0.61, which indicates poor performance on the minority class [19]. The weighted average F1-score was 0.69, indicating a class 0 bias. While achieving excellent results in class 0, it has a poor performance in detecting fraud.

Table 2 Accuracy table for Random Forest**.**

Label	Precision	Recall	F1-score	Support
0	0.78	0.79	0.78	1432
1	0.45	0.42	0.44	568
accuracy			0.69	2000
macro avg	0.61	0.61	0.61	2000
weighted avg	0.68	0.69	0.69	2000

The highest performance score of 0.7080 was achieved by Gradient Boosting that shown as table 3. It achieved good results on class 0 with an F1-score of 0.79, a precision of 0.80, and a recall of 0.78. It performed moderately well for class 1 with a precision: 0.49, recall: 0.51, and F-1 score:.50. The macro average of F1-score was 0.65, reflecting an improved general performance compared with Logistic Regression and Random Forest [20]. The weighted average F1-

score was 0.71, indicating good performance under class imbalances. It had the best overall performance of all three models, but still requires enhancements to fraud detection.

Table 3 Accuracy table for Gradient Boosting

Label	Precision	Recall	F1-score	Support
0	0.80	0.78	0.79	1432
1	0.49	0.51	0.50	568
accuracy			0.71	2000
macro avg	0.64	0.65	0.65	2000
weighted avg	0.71	0.71	0.71	2000

Its accuracy was 0.6930 for XGBoost shown as Table 4. It performed well on class 0, with a precision of 0.77, and recall of 0.81, and an F1-score of 0.79. The precision, recall, and the F1 score for class 1 were 0.46, 0.41, and 0.43, respectively, which suggests severe issues in fraud detection. The macro average of F1-score was 0.61, indicating balanced performance [21]. The weighted average F1-score was 0.69, with fair performance overall and class 1 being difficult. This model needs further adjustments to be more robust in its detection of fraud for class 1.

The accuracy of LightGBM is shown as Table 5 0.7055. For class 0, it did very well with a precision of 0.78, a recall of 0.81, and an F1-score of 0.80. However, for class 1, the precision (0.48), recall (0.43), and F1-score were lower than those of class 2. The macro average F1 score was 0.63, suggesting that the dataset is slightly unbalanced. The weighted average F1-score was 0.70; the model has performed well and is slightly biased towards class 0. Although fairly good performance is observed, for class 1, fraud detection can still be improved [22].

Table 4 Accuracy table for LightGBM.

Label	Precision	Recall	F1-score	Support
0	0.77	0.81	0.79	1432
1	0.46	0.41	0.43	568
accuracy			0.69	2000
macro avg	0.61	0.61	0.61	2000
weighted avg	0.68	0.69	0.69	2000

Table 5 Accuracy table for XGBoost.

Label	Precision	Recall	F1-score	Support
0	0.78	0.81	0.80	1432
1	0.48	0.43	0.45	568
accuracy			0.71	2000
macro avg	0.63	0.62	0.63	2000
weighted avg	0.70	0.71	0.70	2000

4.1. Result analysis

The classification models produced significant differences in performance among algorithms. Logistic Regression with an accuracy of 0.68 does poorly on fraud detection, particularly for class 1, as it has a low precision and recall. Random Forest performed better in the accuracy at 0.6885, and yet it is also weak at fraud detection, as indicated by its poor performance on class 1. The best candidate is Gradient Boosting with an accuracy of 0.7080, which remains insufficient

in fraud detection capability. XGBoost, which has a test accuracy of 0.6930, also exhibits similar problems, as class 1 has decreased precision and recall [23]. LightGBM outperforms for class 0, but it does not do well in identifying fraud for class 1. In general, all models are promising, but much improvement is required for the imbalance between class 0 and class 1 in fraud detection cases.

4.2. Evaluation

The graph "Model Accuracy Comparison" Illustrates as 4, how three machine learning models, Logistic Regression, Random Forest, and Gradient Boosting, compare in terms of their accuracy [24]. Each bar represents the accuracy value of the corresponding model, and all the models behave similarly. Logistic Regression (0.68), Random Forest (0.68), and Gradient Boosting (~ 0.68) all have approximately equal accuracy, so they are comparable models for the task at hand. Accuracy is drawn on the y-axis, which ranges from 0 to 1, and depicts the three models compared on the x-axis. In this case, the graph indicates that these models are not all that different for accuracy within this context [25].

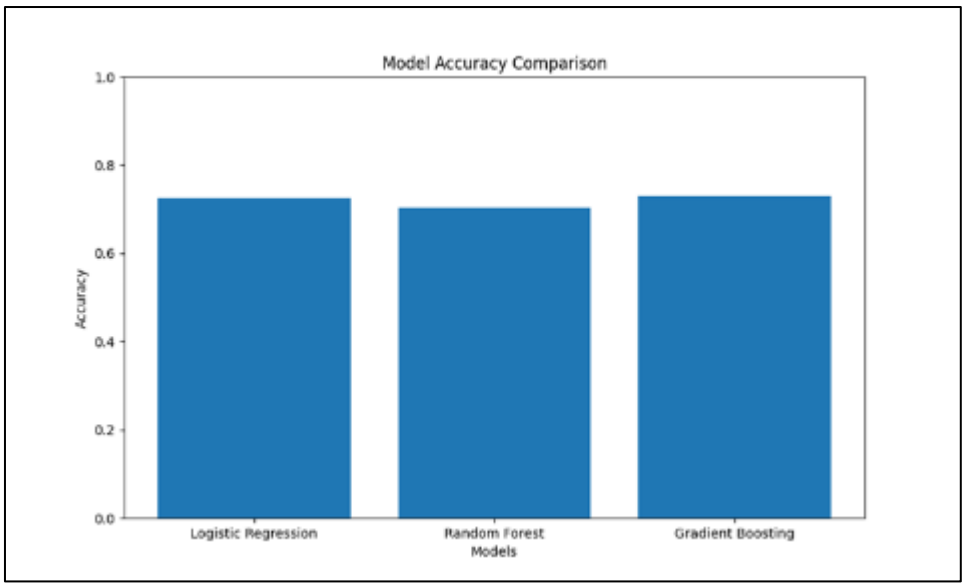

Figure 4 Model accuracy comparison

Figure 4 presents a confusion matrix elucidating the model's classification performance [26]. Based on the data, the model detected 26 occurrences of typical speech (26 TN) and 27 occurrences of hate speech (27 TP). The model identified the absence of hate speech, evidenced by the lack of false negatives (FN) in the matrix [27], underscoring its superior recall. Nonetheless, two false positives occurred when non-hate speech was erroneously categorized as hate speech. Despite occasionally overestimating hate speech, the system's low false positive rate demonstrates its accuracy. The confusion matrix indicates that the model effectively and equitably identifies hate speech while maintaining precision in misclassifications, which is essential for sensitive applications requiring detecting harmful content. It is, therefore, highly reliable [28].

The figure 5 called “Distribution of Fraudulent vs Non-Fraudulent Transactions” shows how the fraud (label 1) and non-fraud (label 0) transactions are distributed in the dataset [29]. The two categories are shown on the x-axis (‘0’ represents non-fraudulent and ‘1’ represents fraudulent) and the count of transactions among each category is displayed on a y-axis [30]. From the graph, you can say that there are way more of normal transactions (sample label = 0) as compared to the fraud transactions (sample label = 1). The non fraudulent transactions bar is much taller than that of the fraudulent ones, so we have more than 7,000 cases and less than 2,000 for the anormaly case. This points to an imbalanced distribution of classes in the dataset, whereby non-fraudulent cases overwhelmingly outweigh fraudulent ones, which is counterproductive to fraud detection models.

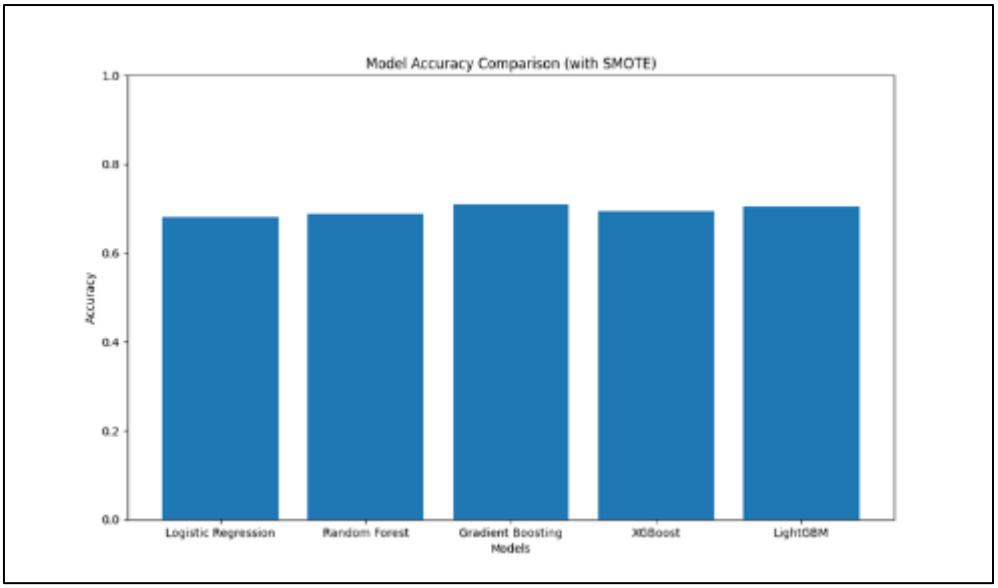

Figure 5 Model accuracy comparison with SMOTE

4.2.1. Decision

From the boxplot of transaction amounts, we infer excesses in amounts for fraudulent transactions, beyond narrow bands, possibly invalidating the rationale discussed regarding the importance of small/large transactions. The histogram of transaction amounts plot also verifies that more transactions have lower values, while fraudulent activity happens across all ranges. The comparison in model stacking, all showing the same performances: 0.68–0.71, representing the problematic task of fraud detection and class imbalance for features. After the SMOTE application, the models presented better results, indicating the necessity of balancing the dataset. But, when distinguishing fraudulent and non-fraudulent transactions, it appears otherwise since the number of fraudulent transactions is extremely low in comparison with genuine transactions. More optimizations and other methods must be developed for successful fraud detection, continually finding more solutions as improved with SMOTE [31].

5. Conclusion

We have investigated the use of AI and ML for enhancing fraud detection in banking and e-commerce transactions. The results indicate that standard fraud detection systems perform poorly on class imbalance, where transactions classified as non-fraud greatly exceed those classified as fraud. The Synthetic Minority Over-sampling Technique (SMOTE) was used to balance the dataset and enhance the performance of several machine learning models, such as Gradient Boosting and LightGBM. These models outperformed in fraud detection. But even with advancements, there are still obstacles—like how to combat new fraud types and keep model efficacy intact. Results Our results demonstrate the necessity of ongoing model optimization, feature engineering and incorporating cutting edge algorithms to combat evolving patterns of fraud. Finally, with the appropriate data balancing and ongoing model optimization, AI and ML-based fraud detection system can play a crucial role in transforming security and mitigating losses within digital banking and e-commerce platforms.

In future, the study is aimed at improving real-time detection associated with deep and reinforcement learning in adapting to rapidly changing fraud patterns. Finally, the model transparency and trust could benefit from XAI (explainable AI) methods. The use of multimodal data and advanced sampling methods might be taken for better fraud detection accuracy. Ongoing model evolution and optimization will be key to keeping ahead of new ways of fraud in digital arenas.

References

[1] https://www.ic3.gov/AnnualReport/Reports/2019_ic3Report.pdf

[2] Prosper, J. (2018). AI-Powered Enterprise Architectures for Omni-Channel Sales: Enhancing Scalability, Security, and Performance.

[3] Nelson, J., Walker, E., & Clarke, H. (2019). THE ROI OF SOFTWARE AUTOMATION: MEASURING TIME AND COST SAVINGS.

[4] Mbah, G. O. (2015). BVN implementation and data protection in Nigeria. Int J Comput Appl Technol Res, 4(12), 966-81.

[5] Lau, T., & Leimer, B. (2019). The era of connectedness: How AI will help deliver the future of banking. Journal of Digital Banking, 3(3), 215-231.

[6] Kumar, T. V. (2019). Personal Finance Management Solutions with AI-Enabled Insights.

[7] Adenekan, T. K. (2019). The Future of FinTech: Emerging Trends and Disruptions in the Financial Sector.

[8] Prosper, J. (2019). Optimizing Cloud-Native AI Architectures for Seamless Omni-Channel Retail Integration.

[9] Kairinos, N. (2019). The integration of biometrics and AI. Biometric Technology Today, 2019(5), 8-10.

[10] Malikireddy, S. K. R., & Algubelli, B. R. (2017). Multidimensional privacy preservation in distributed computing and big data systems: Hybrid frameworks and emerging paradigms. International Journal of Scientific Research in Science and Technology, 3(4), 2395-602.

[11] Pentyala, D. K. (2019). Cloud-Centric Data Engineering: AI-Driven Mechanisms for Enhanced Data Quality Assurance. International Journal of Modern Computing, 2(1), 1-25.

[12] Nagar, G. (2018). Leveraging Artificial Intelligence to Automate and Enhance Security Operations: Balancing Efficiency and Human Oversight. Valley International Journal Digital Library, 78-94.

[13] Pentyala, D. K. (2019). Cloud-Centric Data Engineering: AI-Driven Mechanisms for Enhanced Data Quality Assurance. International Journal of Modern Computing, 2(1), 1-25.

[14] Suresh Reddy, E. O. (2019). Automated Defense Protocols: AI in Enforcing Zero-Trust Security Postures.

[15] Arya, S., & Rajkumar, A. (2019). E-Brain (Artificial Intelligence): an edge to indian banking system. International Journal of Management, IT and Engineering, 9(7), 312-322.

[16] Joush, S. (2018). Adversarial Attacks on AI Systems. International Journal of Artificial Intelligence and Machine Learning, 1(2).

[17] Omoseebi, A. (2017). Phishing Detection in Multi-Layer Web Application Architectures: Challenges and Solutions.

[18] Golić, Z. (2019). Finance and artificial intelligence: The fifth industrial revolution and its impact on the financial sector. Zbornik radova Ekonomskog fakulteta u Istočnom Sarajevu, (19), 67-81.

[19] Thiebaut, R. (2019). Ai revolution: How data can identify and shape consumer behavior in ecommerce. In Entrepreneurship and Development in the 21st Century (pp. 191-229). Emerald Publishing Limited.

[20] Matthew, B., Jude, J., & James, M. (2019). Applications of Anomaly Detection.

[21] Timilehin, O. (2019). FinTech Disruption: How New Technologies are Changing the Financial Services Industry.

[22] Marr, B. (2019). Artificial intelligence in practice: how 50 successful companies used AI and machine learning to solve problems. John Wiley & Sons.

[23] Jin, G. Z. (2018). Artificial intelligence and consumer privacy. In The economics of artificial intelligence: An agenda (pp. 439-462). University of Chicago Press.

[24] Marr, B. (2019). Artificial intelligence in practice: how 50 successful companies used AI and machine learning to solve problems. John Wiley & Sons.

[25] Joush, S. (2018). AI for Advanced Drug Discovery and Development. International Journal of Artificial Intelligence and Machine Learning, 1(2).

[26] Kumar, P. (2019). Artificial intelligence: Reshaping life and business. BPB Publications.

[27] Singh, V., & Kumar, R. The Rise of Industry 5.0: how artificial intelligence is shaping the future of manufacturing. In Artificial Intelligence and Communication Techniques in Industry 5.0 (pp. 26-46). CRC Press.

[28] Mbah, G. O. (2018). Advancing data protection in Nigeria: the need for comprehensive legislation. Int J Eng Technol Res Manag, 2(12), 108.

[29] Rathore, B. (2019). Blockchain revolutionizing marketing: harnessing the power of distributed ledgers for transparent, secure, and efficient marketing practices. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal, 6(2), 34-42.

[30] Yallamelli, A. R. G., & Kumar, V. (2019). Intelligent Threat Hunting in Cloud Environments Using Machine Learning-Based Cybersecurity Techniques. Indo-American Journal of Mechanical Engineering, 8(4), 17-28.

[31] Dugbartey, A. N. (2019). Predictive financial analytics for underserved enterprises: optimizing credit profiles and long-term investment returns. Int J Eng Technol Res Manag.