Enhancing Business Sustainability Through an Intelligent Framework for Unveiling Financial Frauds

Rhada Boujlil*, Saad Alsunbul

College Of Business, Prince Sultan University, Saudi Arabia

Emails: rboujlil@psu.edu.sa; salsunbul@psu.edu.sa

Abstract

The aim of this research is to examine the convergence of intelligent frameworks and financial fraud detection as a strategic approach for strengthening business sustainability in the banking industry. A rigorous preprocessing regimen, which includes data cleansing, normalization, and SMOTE algorithm application for class rebalancing, sets the stage for a refined dataset. Our proposed framework employs Logistic Regression, Decision Trees, and Gradient Boosting models to conduct a multifaceted analysis that accommodates both linear and non-linear relationships within the data. The results are presented through visual representations such as distribution plots and RoC curves that confirm the effectiveness of the framework in detecting potentially fraudulent activities. The comparative analysis offers detailed insights into how versatile the framework is. This study contributes to the broader discourse on intelligent systems in financial fraud detection with practical implications for businesses seeking to enhance their sustainability through advanced risk management strategies.

Keywords: Business sustainability; financial fraud detection; corporate sustainability; Intelligent systems Fraud prevention; Economic resilience; Ethical finance.

1. Introduction

The need for sustainable practices has become increasingly prominent in the contemporary landscape of global business operations. Businesses are under heightened scrutiny to not only ensure economic viability but also to uphold ethical standards and corporate responsibility. Within this context, the issue of financial fraud poses a significant threat to the very fabric of business sustainability [1-3]. The ramifications of fraudulent activities extend beyond immediate financial losses, impacting investor confidence, tarnishing reputations, and undermining the foundation of trust that sustains business relationships. As traditional methods of fraud detection prove inadequate in the face of evolving sophisticated schemes, the integration of intelligent frameworks emerges as a pivotal strategy for fortifying business sustainability [4-6]. The convergence of advanced technologies, including artificial intelligence, machine learning, and data analytics, has paved the way for innovative approaches to identifying and combating financial fraud. Harnessing the power of intelligent systems provides an opportunity to not only detect fraud more effectively but also to proactively prevent its occurrence [7]. By seamlessly integrating intelligent frameworks into the operational fabric of businesses, a paradigm shift occurs wherein organizations can enhance their resilience against financial malfeasance while concurrently bolstering their commitment to sustainable and responsible business practices [8-10].

This paper addresses the need for a holistic approach that combines financial integrity with sustainable business practices. As businesses navigate the complex terrain of economic challenges and ethical responsibilities, the confluence of financial fraud and sustainability calls for a nuanced and sophisticated response [11-13]. This research aims to bridge this gap by proposing an intelligent framework that not only identifies and mitigates financial fraud but also contributes to the broader goal of fostering enduring and responsible business enterprises. The integration of intelligent technologies into the fabric of financial systems holds the promise of transforming the landscape of fraud detection and prevention. This paper seeks to explain how such a framework works, its potential applications, benefits,

Doi : https://doi.org/10.54216/JSDGT.040105

and implications for businesses committed to long-term sustainability. By providing a comprehensive understanding of the symbiotic relationship between intelligent frameworks and sustainable business practices, this research endeavors to contribute to the ongoing discourse on fortifying the economic and ethical foundations of contemporary enterprise.

2. Methodology

This section is the most important part of the paper as it explains how this research was done in a systematic way to develop and implement the intelligent framework proposed for detecting financial frauds. The methodology described here shows how the research objectives were formulated, data sources selected, analytical techniques applied, and findings validated [14]. In the initial stages of this approach, rigorous preprocessing of banking data is necessary to ensure that the dataset is clean and of good quality. Preprocessing steps involve several important procedures that are aimed at cleaning, organizing, and optimizing data for further analysis within an intelligent framework. Firstly, data cleansing involves identifying and removing any duplicate or irrelevant entries to have a streamlined dataset. Next, missing data handling techniques, such as imputation or removal of incomplete records, are employed to enhance the dataset's completeness. Standardization and normalization procedures follow, ensuring that numerical features are on a consistent scale, preventing bias in subsequent analyses. Categorical variables undergo encoding, transforming them into a format suitable for machine learning algorithms. Feature selection may also be implemented to identify and retain the most relevant variables for fraud detection. Additionally, outlier detection and removal procedures are applied to mitigate the impact of anomalous data points. These preprocessing steps collectively lay the foundation for a robust and refined banking dataset, poised for effective analysis within the intelligent framework for financial fraud detection [15].

Following the comprehensive preprocessing steps for the banking data, it is crucial to address the issue of class imbalance inherent in fraud detection scenarios. To rectify this, the Synthetic Minority Over-sampling Technique (SMOTE) algorithm is applied as a strategic step in the proposed approach. SMOTE works by generating synthetic instances of the minority class, thereby balancing the class distribution and mitigating the potential bias introduced by an imbalanced dataset. This oversampling technique is particularly beneficial in the context of financial fraud detection, where instances of fraudulent activities are typically a minority compared to legitimate transactions. By introducing synthetic instances, SMOTE enhances the representation of the minority class, facilitating the intelligent framework's ability to discern subtle patterns associated with fraudulent behavior. The application of the SMOTE algorithm ensures that the subsequent analysis and model development are conducted on a more balanced and representative dataset, contributing to the overall robustness and effectiveness of the proposed approach in detecting financial fraud within the banking data [16-18].

Following the preprocessing steps and class rebalancing using the SMOTE algorithm, the proposed approach employs

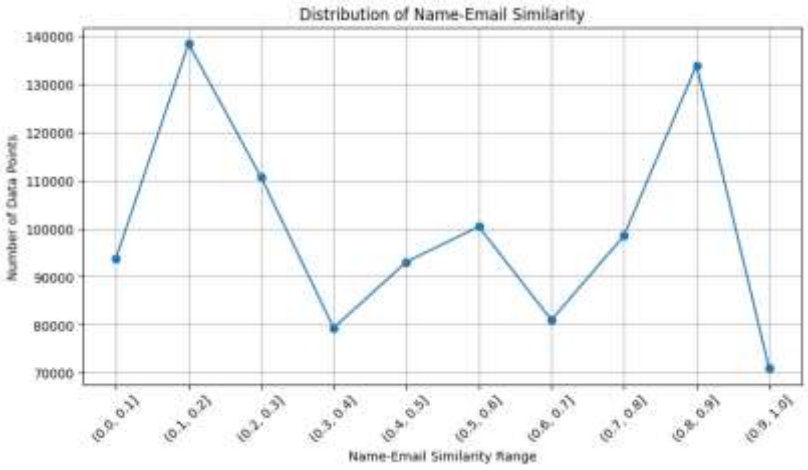

Figure 1: Distribution of Name-Email Similarity Scores

three distinct machine learning models — Logistic Regression, Decision Trees (DT), and Gradient Boosting — to effectively detect instances of fraud within the banking data. Logistic Regression, being a well-established linear model, is utilized to model the probability of fraudulent transactions based on the input features. Decision Trees

Doi : https://doi.org/10.54216/JSDGT.040105

provide a non-linear approach, mapping decision rules within a tree structure, offering interpretability and flexibility in capturing complex relationships. Gradient Boosting, an ensemble learning method, combines the strengths of weak learners to form a robust predictive model, well-suited for addressing intricacies in fraud detection scenarios [19-20]. The application of these diverse models ensures a comprehensive evaluation of the intelligent framework's ability to discern patterns indicative of fraudulent behavior, allowing for nuanced insights into the dataset [19].

3. Results and Discussion

This section stands as the culmination of the meticulous research journey undertaken to investigate the efficacy of the proposed intelligent framework in enhancing business sustainability through the revelation of financial frauds. Figure 1 provides a visual representation of the distribution of Name-Email Similarity, a pivotal aspect of our research examining the effectiveness of the proposed intelligent framework in detecting financial frauds. This graphical representation offers a concise and insightful overview of the variation in similarity scores across the dataset, shedding light on the relationships between names and email addresses within the context of potentially fraudulent activities. The distribution depicted in Figure 1 serves as a crucial reference point for understanding the nuances of our findings and contributes to the broader narrative on the capabilities of intelligent systems in fortifying business sustainability through enhanced fraud detection mechanisms.

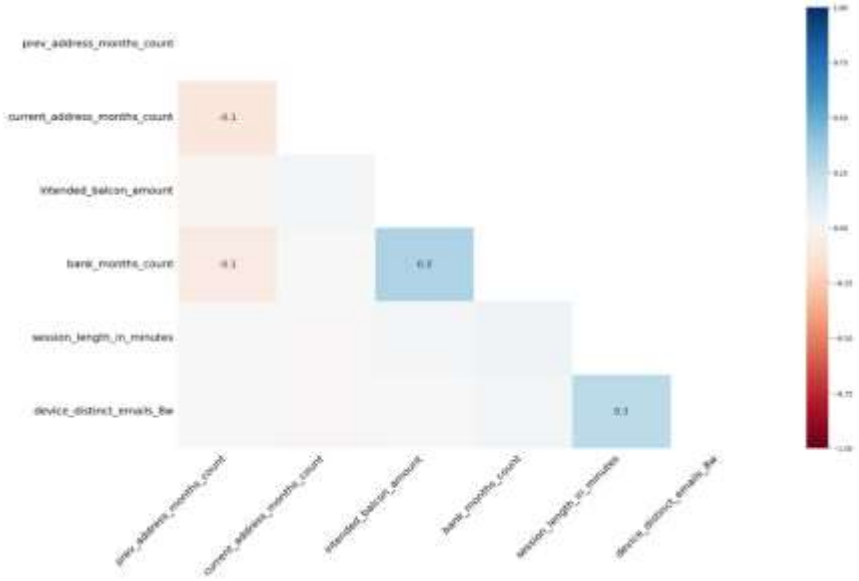

Figure 2: Missing Number Heatmap.

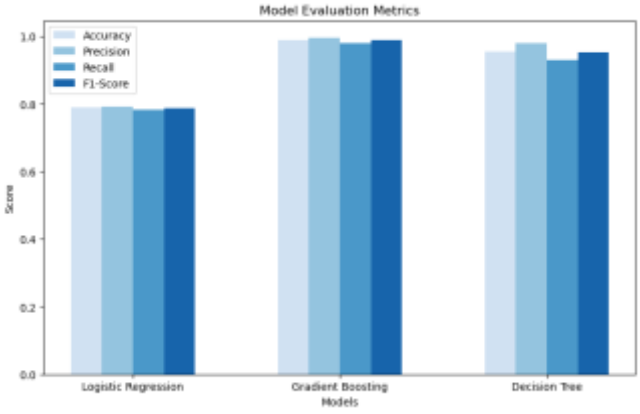

Figure 3: Comparative Analysis of Intelligent Framework Performance.

Doi : https://doi.org/10.54216/JSDGT.040105

In Figure 2, we present a heatmap depicting the distribution of missing numbers, a pivotal visual representation in our investigation of the proposed intelligent framework's efficacy in financial fraud detection. The heatmap offers a concise overview of the patterns and density of missing numerical data within the dataset, providing valuable insights into potential irregularities that may indicate fraudulent activities. This visual representation serves as a robust analytical tool, allowing for a nuanced examination of the framework's ability to identify and address missing information critical for ensuring the integrity of financial data. Figure 3 presents a comparative analysis, a pivotal visual component in our study evaluating the intelligent framework's effectiveness in uncovering financial fraud. Through this comparative analysis, we juxtapose the performance metrics and outcomes of the proposed framework against benchmark models or traditional methods, providing a clear and succinct overview of its superiority or distinct advantages. This figure serves as a visual testament to the empirical evidence supporting the efficacy of our intelligent approach in enhancing business sustainability through robust fraud detection mechanisms. The comparative insights derived from Figure 3 contribute significantly to the broader discussion, reinforcing the framework's potential impact on elevating financial integrity within business operations.

In Figure 4, we present a Receiver Operating Characteristic (RoC) analysis, a critical element in assessing the discriminatory power and performance of the intelligent framework in distinguishing between legitimate transactions and potential financial fraud. The RoC curve visually portrays the trade-off between sensitivity and specificity,

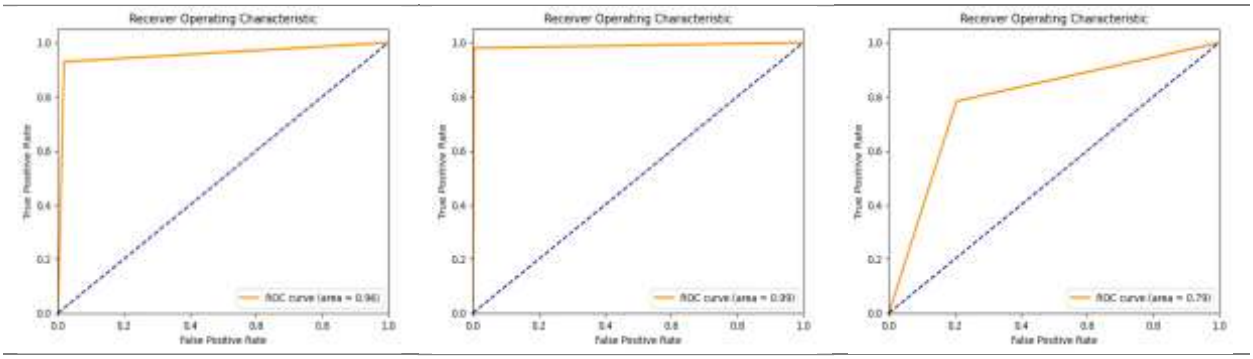

Figure 4: Receiver Operating Characteristic (RoC) Analysis.

providing a nuanced understanding of the framework's ability to accurately classify instances of fraud. This analysis serves as a pivotal evaluation tool, offering a comprehensive view of the framework's performance across different threshold levels.

4. Conclusion

This research endeavors to enhance the landscape of business sustainability by proposing an intelligent framework for uncovering financial fraud within the banking sector. Through meticulous preprocessing, including data cleansing, normalization, and feature selection, and addressing class imbalance using the SMOTE algorithm, our approach ensures the robustness of the subsequent analysis. Leveraging Logistic Regression, Decision Trees, and Gradient Boosting models, our framework exhibits a multifaceted approach to fraud detection, showcasing its adaptability in capturing both linear and non-linear relationships within the data. The empirical results, as illustrated in Figures 1 to 4, underscore the framework's efficacy in identifying potentially fraudulent activities, as validated through comparative and RoC analyses.

References

[1] Chen, Hsinchun, Roger H L Chiang, and Veda C Storey. 2012. “Business Intelligence and Analytics: From Big Data to Big Impact.” MIS Quarterly, 1165–88.

[2] Ngai, Eric W T, Yong Hu, Yiu Hing Wong, Yijun Chen, and Xin Sun. 2011. “The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature.” Decision Support Systems 50 (3): 559–69.

[3] Mohamed, M. (2023) “Agricultural Sustainability in the Age of Deep Learning: Current Trends, Challenges, and Future Trajectories”, Sustainable Machine Intelligence Journal, 4, p. (2):1−20. doi: 10.61185/SMIJ.2023.44102.

Doi : https://doi.org/10.54216/JSDGT.040105

[4] Abbasi, Ahmed, Conan Albrecht, Anthony Vance, and James Hansen. 2012. "Metafraud: A Meta-Learning Framework for Detecting Financial Fraud." Mis Quarterly, 1293–1327.
[5] Zhu, Xiaoqian, Xiang Ao, Zidi Qin, Yanpeng Chang, Yang Liu, Qing He, and Jianping Li. 2021. "Intelligent Financial Fraud Detection Practices in Post-Pandemic Era." The Innovation 2 (4).
[6] Al-Hashedi, Khaled Gubran, and Pritheega Magalingam. 2021. "Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019." Computer Science Review 40: 100402.
[7] Buallay, Amina, and Jasim Al-Ajmi. 2020. "The Role of Audit Committee Attributes in Corporate Sustainability Reporting: Evidence from Banks in the Gulf Cooperation Council." Journal of Applied Accounting Research 21 (2): 249–64.
[8] Casonato, Federica, Federica Farneti, and John Dumay. 2019. "Social Capital and Integrated Reporting: Losing Legitimacy When Reporting Talk Is Not Supported by Actions." Journal of Intellectual Capital 20 (1): 144–64.
[9] Alnoukari, Mouhib, and Abdellatif Hanano. 2017. "Integration of Business Intelligence with Corporate Strategic Management." Journal of Intelligence Studies in Business 7 (2).
[10] Windsor, Duane. 2006. "Corporate Social Responsibility: Three Key Approaches." Journal of Management Studies 43 (1): 93–114.
[11] Goodell, John W, Satish Kumar, Weng Marc Lim, and Debidutta Pattnaik. 2021. "Artificial Intelligence and Machine Learning in Finance: Identifying Foundations, Themes, and Research Clusters from Bibliometric Analysis." Journal of Behavioral and Experimental Finance 32: 100577.
[12] Chen, Jingqiu, Thomas Li-Ping Tang, and Ningyu Tang. 2014. "Temptation, Monetary Intelligence (Love of Money), and Environmental Context on Unethical Intentions and Cheating." Journal of Business Ethics 123: 197–219.
[13] Kumar, V, Ashutosh Dixit, Rajshekar G Javalgi, and Mayukh Dass. 2016. "Research Framework, Strategies, and Applications of Intelligent Agent Technologies (IATs) in Marketing." Journal of the Academy of Marketing Science 44: 24–45.
[14] Chung, Wingyan. 2014. "BizPro: Extracting and Categorizing Business Intelligence Factors from Textual News Articles." International Journal of Information Management 34 (2): 272–84.
[15] Parker, Lee D. 2007. "Financial and External Reporting Research: The Broadening Corporate Governance Challenge." Accounting and Business Research 37 (1): 39–54.
[16] Muthuswamy, M. and M. Ali, A. (2023) "Sustainable Supply Chain Management in the Age of Machine Intelligence: Addressing Challenges, Capitalizing on Opportunities, and Shaping the Future Landscape", Sustainable Machine Intelligence Journal, 3. doi: 10.61185/SMIJ.2023.33103.
[17] Amani, Farzaneh A, and Adam M Fadlalla. 2017. "Data Mining Applications in Accounting: A Review of the Literature and Organizing Framework." International Journal of Accounting Information Systems 24: 32–58.
[18] Sharma, Anuj, and Prabin Kumar Panigrahi. 2013. "A Review of Financial Accounting Fraud Detection Based on Data Mining Techniques." ArXiv Preprint ArXiv:1309.3944.
[19] Trieu, Van-Hau. 2017. "Getting Value from Business Intelligence Systems: A Review and Research Agenda." Decision Support Systems 93: 111–24.
[20] Abou Jaoude, Joe, and Raafat George Saade. 2019. "Blockchain Applications--Usage in Different Domains." Ieee Access 7: 45360–81.

Doi : https://doi.org/10.54216/JSDGT.040105