IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13920

Systematic Review of Real-Time Analytics and Artificial Intelligence Frameworks for Financial Fraud Detection

Oluwatofunmi O. Oguntibeju[1], Michael Adonis[2], John Alade[3]

Senior Engineer, Andela, New York, USA[1]

Senior Engineer, Andela, New York, USA [2]

Engineer, MTN Telecommunications[3]

Abstract: The technological advancement of the financial industry has been vital in ensuring that it is more accessible to consumers. Still, it has also brought up complicated security issues, such as financial fraud. Conventional rule-based fraud detection methods consistently have challenges in staying up with the speed at which cyber threats evolve. To solve these issues, this systematic study examines how real-time analytics and artificial intelligence (AI) frameworks might improve the detection of fraud capabilities. Prior research has concentrated on discrete AI models but has frequently needed more thorough integration with real-time data. This review addresses the gaps in previous research by analyzing various AI models, including neural networks, support vector machines, and graph-learning algorithms in the context of identifying fraudulent behavior. The paper assesses experimental settings and real-world applications, offering insights into various frameworks' efficacy, scalability, and adaptability in real-time financial situations. This research also contributes to financial fraud detection systems continuous growth by investigating how AI-powered techniques might improve fraud detection accuracy, precision, and reaction times. Additionally, combining AI with real-time analytics is a viable way to combat the growing complexity of criminal activities related to financial crime.

Keywords: Real-Time Analytics, Artificial Intelligence, Financial Fraud Detection, Machine Learning, Fraudulent Transactions, Supervised Learning, Unsupervised Learning, Data Mining, Graph, Learning Algorithms, Explainable AI (XAI)

I. INTRODUCTION

The digital transformation of the banking sector has been vital in transforming the accessibility and ease for consumers throughout the globe. Nevertheless, there are difficulties since traditional rule-based fraud detection techniques have found it challenging to keep up with the quick growth of cyber threats. This has driven interest in more flexible methods like unsupervised learning [6]. Previous studies focused on the effectiveness of several AI models in identifying fraudulent activity, which left a gap as they frequently concentrated on discrete frameworks or did not provide a thorough assessment of the integration of real-time analytics with AI. Building on previous studies, this systematic study examines ways in which real-time analytics and AI frameworks may function together to close that gap and provide a more comprehensive method of detecting and dealing with fraud.

In the modern age of enormous amounts of data, manual detection methods based on traditional approaches are time-consuming, costly, and incorrect and need to be more workable [11]. This highlights the need for more study to overcome the shortfalls of current frameworks and investigate the new approaches that use artificial intelligence (AI) and real-time analytics. More research is required since earlier studies' findings about the flexibility and scalability of AI in fraud detection were varied. It aims to systematically analyze and improve the approaches used in AI-driven financial fraud detection.

II. LITERATURE REVIEW

Artificial intelligence (AI), machine learning, and statistical methods have been used in recent developments in financial fraud detection to improve accuracy and efficiency. Danenas identified important characteristics of contemporary fraud detection systems and emphasized the emergence of intelligent solutions [5]. After conducting a thorough study, Al-Hashedi and Magalingam [1] found that over 81% of relevant research used data mining techniques, mainly in the context of banking and insurance fraud. To improve fraud detection skills, Li [9] presented the graph-learning algorithm TA-Struc2Vec, which creatively collects topological and transaction characteristics in financial networks. This study journal will build on using these systems to apply accurate time analytics and artificial intelligence frameworks for financial fraud detection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13920

III. HYPOTHESES AND THEIR CORRESPONDENCE TO RESEARCH DESIGN

The study's primary hypothesis is that when real-time analytics and AI frameworks are combined, financial fraud detection becomes far more accurate and efficient than it would be with traditional methods. The secondary hypothesis, however, suggests that some AI methods, such as graph-learning algorithms and unsupervised learning, offer better scalability and flexibility in dynamic financial contexts. Such concepts show the necessity for sophisticated, data-driven cybersecurity techniques based on accepted frameworks.

The study design aligns with these hypotheses by methodically examining actual research and case studies on AI-driven fraud detection, emphasizing real-time capabilities. In terms of practical implications, the study can help financial institutions build more reliable and scalable fraud detection systems by verifying the function of AI in enhancing fraud detection. This structure allows for a thorough analysis of the theories and serves as a foundation for further study in this developing study area.

IV. METHODOLOGY

A. *Subject characteristics*

The studies eligible for inclusion in this review had to fulfill three requirements: be published in English, offer empirical data or simulations, and concentrate on real-time analytics or AI-based frameworks for financial fraud detection. Studies that dealt with fraud in non-financial fields or were exclusively theoretical, without any application or assessment, were excluded.

B. *Data Sources and Search Strategy*

A conclusive search on the literature review was done using various electronic databases, such as PubMed, IEEE Xplore, Scopus, and Google Scholar. Keywords including "real-time analytics," "artificial intelligence," "machine learning," "financial fraud detection," and "fraudulent transactions" were part of the search strategy. Research released between 2000 and 2024 in proceedings of conferences, experimental studies, and peer-reviewed journals was taken into consideration.

C. Sampling Procedures

Our goal was to combine some publications from different sources for this systematic review to include empirical research on real-time analytics and artificial intelligence frameworks for financial fraud detection. We reviewed 5 papers that met our criteria. This sample size captured a variety of techniques and application situations, offering solid insights into the usage of AI in financial fraud detection. Nevertheless, differences in sample sizes, reporting requirements, and research quality across the chosen studies could have impacted our results' accuracy and ability for generalization. This research evaluated the usefulness of real-time analytics and AI frameworks in identifying financial fraud using metrics including accuracy, precision, recall, and F1-score as the primary outcome measure. Processing time, scalability, and the rates of false positives and false negatives were among the additional outcome measures.

This review considered studies using both experimental and observational research methodologies. Most research used experimental designs, in which real-time analytics frameworks or AI models were implemented in fictitious financial contexts, and their efficacy in identifying fraudulent activity was evaluated. Observational designs were employed in specific research to assess the efficacy of AI frameworks without manipulating real-world transaction data.

V. RESULTS

Table 1 below shows results from the first paper reviewed by Kamuangu [7], which examined cutting-edge methods for combating financial fraud with an emphasis on the efficiency of artificial intelligence (AI) and machine learning (ML).

Table 1: Supervised algorithm, AI for fraud detection

Supervised Algorithm	Accuracy	Precision	F1 score	Recall
Logistic Regression	0.92	0.89	0.85	0.87
Decision Trees	0.94	0.91	0.88	0.89
SVM	0.93	0.90	0.87	0.88
GBM	0.95	0.93	0.91	0.92

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13920

The paper examining the real-world dataset from their industrial partner, which included 197,471 transactions over three months, was included. The ordinate below from Mekterović [10] displays the actual fraud rate. In contrast, the abscissa displays the rank, or the total number of transactions arranged according to the likelihood of fraud.

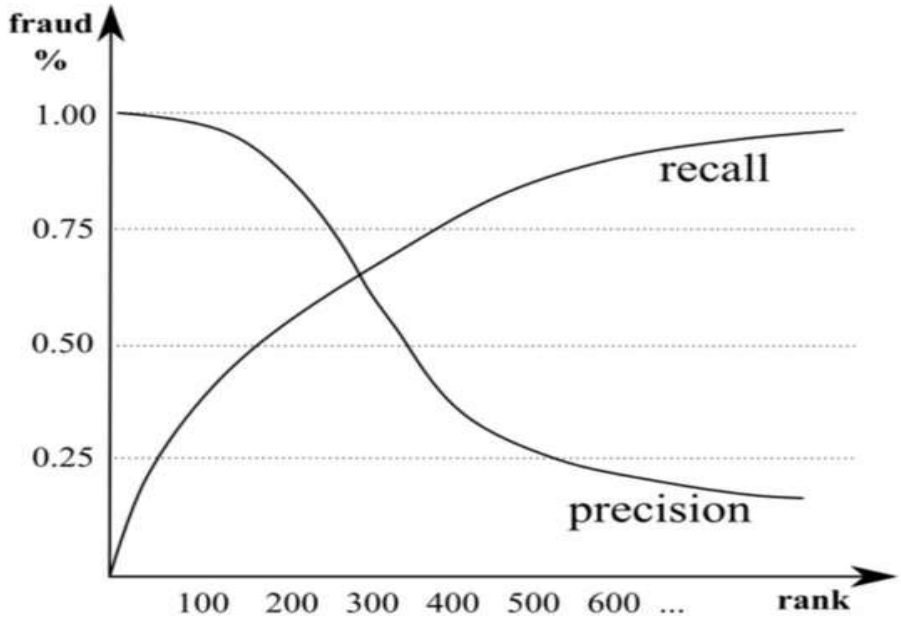

Figure 1: Precision recall charts for fraud rates

According to the studies from a systematic review by Ali [2], the most common types of fraud in the literature include credit card fraud and neural networks (NN and SVM), which are prominent machine learning techniques used for fraud. In 2015, the study was carried out in Korea using accurate payment data from an IoT context [4]. Experiments showed that most algorithms use the public dataset to provide the F-measure value using the suggested choice of features procedure. The figure below demonstrates it, and after deciding on features in a public dataset, the techniques based on unsupervised learning had a maximum accuracy rise of 11.5% and an average of around 11%.

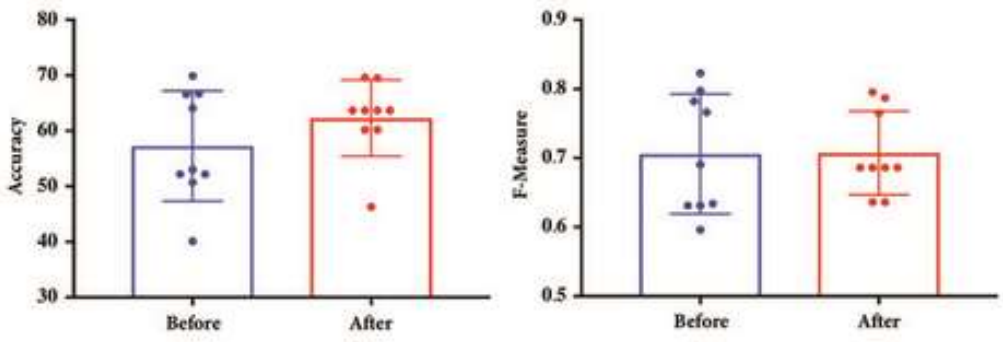

Figure 2: Application of a new model for fraud detection

Peer review journal by Bello [3] shows that getting feedback from their activities and reinforcement learning algorithms enhances detection tactics and makes better decisions over time. As fresh transaction data becomes available, online learning algorithms gradually update the models to keep them responsive and up to date. Rapid identification and reaction to questionable transactions are made possible by real-time data processing capabilities, significantly lowering the possibility of monetary losses. Furthermore, by using explainable AI (XAI) approaches, these models' decision-making processes are made public and comprehensible, promoting confidence and compliance with legal standards. Addressing these issues is necessary for implementing adaptive machine-learning models for real-time fraud prevention.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024
DOI: 10.17148/IJARCCE.2024.13920

VI. DISCUSSION

The research's findings validate the central hypothesis that the combination of real-time analytics and AI frameworks dramatically improves the precision and efficacy of financial fraud identification compared to conventional methods. Supervised models, such as Gradient Boosting Machines, demonstrated high precision and recall rates, confirming the theoretical advantage of AI integration. Conversely, the secondary hypothesis is only partially supported, as some AI models, such as unsupervised learning, showed promise, but their ability to scale in dynamic contexts remains a challenge. Some limitations are mentioned, such as biased dataset selection and inconsistent reporting guidelines. Nevertheless, the results highlight the usefulness of AI in immediate fraud detection and call for more research on evolving and scalable models.

VII. CONCLUSION

The transformational potential of combining real-time data with AI frameworks to greatly improve financial fraud detection is highlighted by this systematic review. The study confirms that AI may significantly increase detection efficacy and precision, and it recommends more research into developing and scalable AI models. The study indicates the need for more research to address constraints such as dataset biases and scalability issues of unsupervised learning models, even if it supports the main idea. Further research should concentrate on improving AI methods and growing datasets to improve fraud detection systems' precision and flexibility. Strong, real-time detection technologies will require ongoing innovation and empirical validation as financial fraud changes.

REFERENCES

[1]. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.
[2]. 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.
[3]. Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: real-time financial fraud prevention concepts in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(2), 021–034.
[4]. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation: SecuritySecurity and Communication Networks, 2018(1), 5483472.
[5]. Danenas, P. (2015). Intelligent financial fraud detection and analysis: a survey of recent patents. Recent Patents on Computer Science, 8(1), 13–23.
[6]. Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. The American Journal of Management and Economics Innovations, 6(06), 8-22.
[7]. Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine
[8]. Learning. Journal of Economics, Finance and Accounting Studies, 6(1), 67-77.
[9]. Li, R., Liu, Z., Ma, Y., Yang, D., & Sun, S. (2022). Internet financial fraud detection based on graph learning. IEEE Transactions on Computational Social Systems, 10(3), 1394-1401.
[10]. Mekterović, I., Karan, M., Pintar, D., & Brkić, L. (2021b). Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest? Applied Sciences, 11(15), 6766. https://doi.org/10.3390/app11156766
[11]. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & Security, pp. 57, 47–66.

