Applications of Artificial Intelligence in Financial Risk Assessment and Fraud Prevention

تطبيقات الذكاء الاصطناعي في تقييم المخاطر المالية ومنع الاحتيال

Hatem Khater
Dean of Faculty of Engineering
Horus University Egypt, New Damiatta, Damiatta, Egypt.

مجلة منارة الإسكندرية للعلوم التجارية – دورية علمية محكمة
(ISSN/O : 3062 – 5548) - (ISSN/P :3062 -5696)

مجلة منارة الإسكندرية للعلوم التجارية

Applications of Artificial Intelligence in Financial Risk Assessment and Fraud Prevention

تطبيقات الذكاء الاصطناعي في تقييم المخاطر المالية ومنع الاحتيال

Hatem Khater
Faculty of Engineering, Horus University Egypt, New Damiatta, Damiatta, Egypt.
Hatem.a.khater@gmail.com

This study investigates how artificial intelligence (AI) can improve financial risk assessment and fraud prevention. Traditional rule-based systems are failing to identify complex fraud patterns and manage dynamic risk profiles as a result of the growing volume and complexity of financial transactions. Machine learning (ML), deep learning (DL), and natural language processing (NLP) are three examples of AI technologies that provide scalable, real-time solutions that can analyze large datasets, spot anomalies, and generate precise predictions. The study examines recent approaches, case studies, and uses of AI in financial institutions, such as insider trading detection, credit scoring, and anti-money laundering. It also draws attention to the expanding application of explainable AI (XAI) to resolve issues with regulatory compliance and model transparency. Even with the notable gains in accuracy and efficiency, issues with algorithmic bias, data privacy, and ethical responsibility still exist. The study comes to the conclusion that although AI has the potential to completely transform financial systems, its effective integration necessitates strong governance frameworks, interdisciplinary cooperation, and ongoing innovation to guarantee security, fairness, and confidence.

Key Words: Artificial Intelligence, Financial, Risk Management, Fraud Detection

المستخلص العربى

يبحث هذا البحث في كيفية إحداث الذكاء الاصطناعي تحولاً في إدارة المخاطر المالية وكشف الاحتيال. ويوضح كيف تُتاح إمكانية الكشف عن الحالات الشاذة والتنبؤ بها وتحليلها آنياً من خلال أدوات الذكاء الاصطناعي، مثل التعلم الآلي والتعلم العميق ومعالجة اللغة الطبيعية، والتي تُحدث ثورة في الأنظمة المالية التقليدية. ويتناول البحث الأبحاث والمنهجيات والأمثلة الحالية، مع تناول الآثار الأخلاقية والقانونية لاعتماد الذكاء الاصطناعي في القطاع المالي. وتُظهر النتائج أنه على الرغم من التحسينات الملحوظة التي يُقدمها الذكاء الاصطناعي في الدقة والكفاءة، إلا أن المشاكل المتعلقة بإمكانية تفسير النماذج وخصوصية البيانات والامتثال لا تزال قائمة.

Introduction

Artificial Intelligence (AI) integration is causing a significant transformation in the financial services sector. Traditional rule-based systems find it difficult to keep up with changing risk profiles and evolving fraud tactics as financial transactions grow more complicated and extensive [1]. Artificial intelligence (AI) technologies, particularly machine learning (ML), deep learning (DL), and natural language processing (NLP), provide scalable and adaptable solutions that can instantly analyze large datasets, uncover hidden patterns, and make highly accurate predictions [2].

Recent advancements in generative AI, transformer-based models, and Graph Neural Networks (GNNs) have further improved the capabilities of AI systems in financial contexts by enabling better outlier detection and more nuanced comprehension of unstructured data [3].
AI is currently being used by financial institutions for operational risk management, insurance underwriting, anti-money laundering (AML), fraud detection, and credit scoring [4]. Concerns about model transparency and legal compliance are being addressed by the growing adoption of explainable AI (XAI) systems [3].

Notwithstanding these developments, algorithmic bias, data governance, and ethical accountability are some of the new issues brought about by the use of AI. AI systems must be fair, secure, and interpretable according to regulations like GDPR and Basel III [5]. Financial institutions should strike a balance between innovation and accountability as AI develops further to ensure operational resilience and trust [6].

(ISSN/ O : 3062 – 5548) - (ISSN/ P : 3062 – 5696)

The complexity and volume of transactions are increasing, making it harder for financial institutions to detect fraud and manage risk. When it comes to recognizing complex fraud patterns and adjusting to emerging threats, traditional rule-based systems frequently fail [16]. By using data-driven methods to improve operational efficiency and decision-making, artificial intelligence (AI) offers a practical solution. With an emphasis on machine learning, deep learning, and natural language processing technologies, this paper investigates the use of AI in financial risk management and fraud detection.

2. Literature Review

Statistical methods and expert-driven rule systems were key components of early financial risk management and fraud detection strategies [7]. Despite being fundamental, these techniques were not flexible enough to take advantage of unstructured data sources or adjust to new fraud trends. With ML algorithms that can learn from past data and adjust to changing conditions, the field has advanced significantly with the rise of AI [8].

In high-dimensional and sequential data environments, deep learning models such as transformers, Long Short-Term Memory (LSTM) networks, and Convolutional Neural Networks (CNNs) have demonstrated exceptional efficacy in identifying fraudulent transactions [6]. By enabling the analysis of textual data from financial disclosures, social media, and emails, natural language processing (NLP) has improved the detection of reputational and insider trading risks [9][33][36].

The increasing efficacy of DL models in financial fraud detection, particularly in managing unbalanced datasets and enhancing feature engineering, is demonstrated by a comprehensive literature review of 57 studies conducted between 2019 and 2024 [6][34]. Because of their capacity to adjust to intricate fraud scenarios, hybrid models that combine supervised, unsupervised, and reinforcement learning techniques are becoming more and more popular [3][28][35].

Nonetheless, there are still issues with addressing ethical issues, guaranteeing model transparency, and adhering to changing data privacy laws. To improve security and accountability, the combination of blockchain technology with privacy-preserving methods such as Principal Component Analysis (PCA) is being investigated [6].

These advancements highlight the necessity of interdisciplinary cooperation and robust governance frameworks when implementing AI in finance.

In the past, rule-based systems and statistical models were used by financial institutions to evaluate risk and identify fraud [7]. More adaptable and scalable methods have been introduced by recent developments in AI. While deep learning models, such as neural networks, have demonstrated superior efficacy in complex classification tasks, machine learning algorithms can learn from historical data to identify patterns [1]. Analysis of unstructured data, such as emails and transaction descriptions, is made possible by natural language processing [9]. Notwithstanding these developments, issues with instantaneous deployment and model interpretability still exist [11][29].

3. Methodology Based on Machine Learning

3.1 AI Techniques

Two techniques are used in machine learning to predict future outcomes: supervised learning, which involves training a model on known input and output data, and unsupervised learning, which involves identifying hidden patterns or internal structures in input data, as illustrated in figure 1. This study examines artificial intelligence (AI) methods used on financial datasets, such as transaction histories, client profiles, and past fraud cases. Risk scoring is done using supervised learning techniques like logistic regression and random forests [8][31], and outlier detection is done using unsupervised learning techniques like clustering and autoencoders [17][32]. Textual data is analyzed by NLP models to identify fraudulent communication and insider trading. Metrics such as precision, recall, F1-score, and ROC-AUC are used to evaluate the efficacy of the model [13][30].

3.2 Supervised Learning

For risk scoring, supervised learning techniques such as Random Forests and Logistic Regression are employed. To forecast the possibility of fraud or financial risk, these models are trained on labeled datasets.

3.3 Unsupervised Learning

For outlier detection, unsupervised learning methods such as autoencoders and clustering are employed. These models are useful for spotting new fraud cases because they can spot odd patterns in data without the need for labeled examples.

3.4 Natural Language Processing (NLP)

Textual data such as emails, social media posts, and financial disclosures are analyzed by NLP models. By spotting questionable linguistic patterns, they are employed to identify insider trading and fraudulent communication.

3.5 Evaluation Metrics

The effectiveness of AI models is assessed using the following metrics: Accuracy: Shows the overall accuracy of a prediction. Precision: Indicates the percentage of predicted frauds that were actually frauds. Recall: Shows the percentage of actual frauds that were correctly identified. The harmonic mean of recall and precision is known as the F1-score. ROC-AUC: Assesses the model's capacity to differentiate between instances of fraud and those that are not.

3.6 Summary of the Flow

As seen in Figure 2, gathering data from multiple financial sources is the first step in the AI methodology. Depending on the task, this data is then processed using various AI techniques, such as NLP for textual analysis, supervised learning for prediction, and unsupervised learning for outlier detection. Lastly, to ensure effectiveness and dependability, the models are evaluated using common effectiveness metrics.

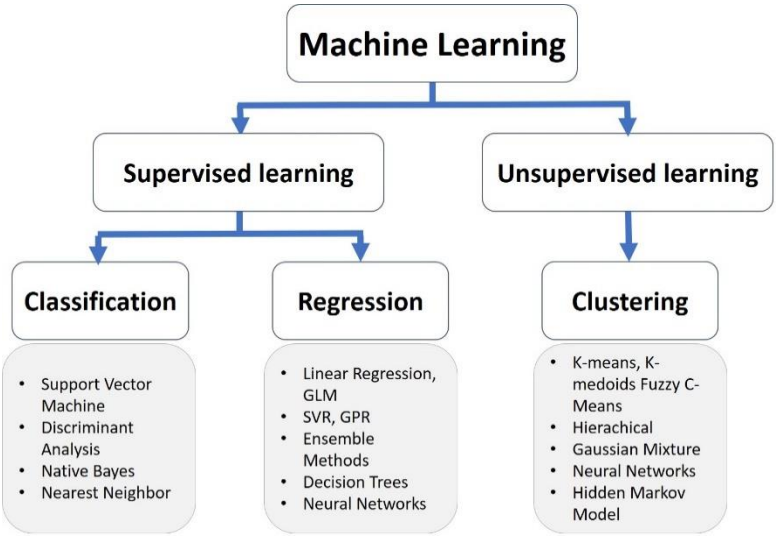

Figure 1: Methods of machine learning [18]

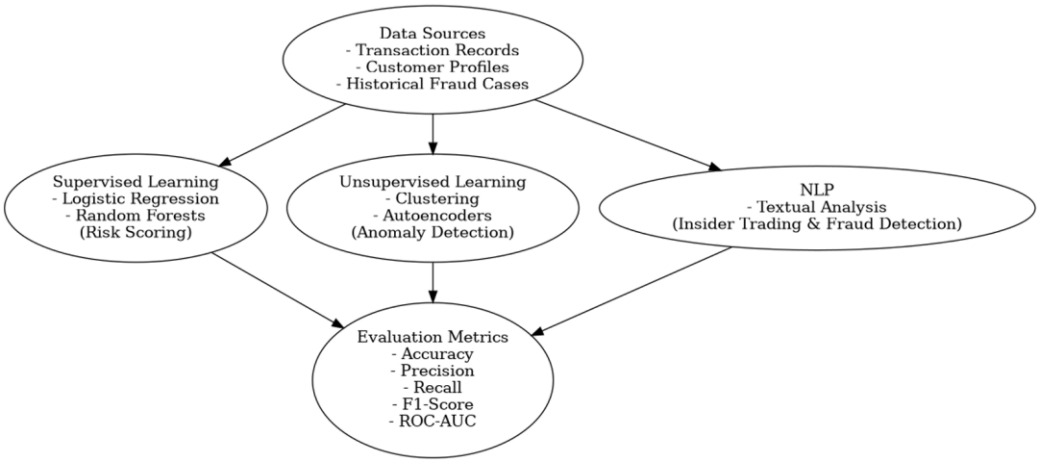

Figure 2: Fraud Detection Framework Using Machine Learning Techniques [19]

3.7 Dataset

The Fraud Detection Dataset on Kaggle is a popular dataset for research on financial fraud detection [26]. The following are included in this dataset: • Transaction Amount: The total amount of money exchanged.

• Transaction Time: A timestamp that shows the exact moment the transaction took place.
• Customer ID: A customer's anonymized identification number.
• Merchant Category: The kind of business or merchant.
• Fraud Label: A binary indicator with 1 denoting fraud and 0 denoting legitimacy.

Using metrics like precision, precision, recall, and ROC-AUC, the dataset—which comprises 594,643 transactions from 4,112 users—is frequently used to train and evaluate machine learning models [27].

4. Case Studies / Applications

Numerous financial applications have successfully incorporated AI. For example, high-precision credit card fraud detection has been achieved using deep learning models [14]. By examining news articles and social media, natural language processing (NLP) techniques have been used to detect insider trading [13].

Predictive models are used in risk management to optimize portfolio risk and evaluate loan default probabilities [2]. These uses demonstrate how AI can improve decision-making and financial security.

4.1. Comparative Case Studies

4.1.1 JP Morgan – COiN (Contract Intelligence)

The COiN platform was created by JP Morgan to use Natural Language Processing (NLP) to automate the review of legal documents. Every year, the system saves about 360,000 hours of manual labor by processing over 12,000 contracts in a matter of seconds [20].

4.1.2 PayPal – AI-Powered Fraud Detection

PayPal uses deep learning models to quickly identify fraudulent transactions. By analyzing billions of transactions, these models increase the accuracy of fraud prevention and decrease false positives [21].

4.1.3 Deutsche Bank – Trade Settlement Automation

Google Cloud and Deutsche Bank are working together to automate trade settlements through the use of generative AI. This program increases back-office productivity and gives analysts real-time insights [22].

4.1.4 SmartDev – AI for Credit Reporting

SmartDev analyzes data from other sources, such as utility payments and mobile usage, using artificial intelligence. By creating credit scores for underbanked groups, this strategy encourages financial inclusion [23].

4.1.5 Morgan Stanley – AI for Financial Advisors

To help financial advisors, Morgan Stanley has implemented chatbots driven by OpenAI. These bots increase productivity, produce client documentation, and conduct investment research [24].

4.1.6 Upstart – AI for Loan Underwriting

Upstart evaluates loan risk more precisely than conventional credit scoring systems by using AI models. This preserves risk standards while increasing loan approval rates [25].

5. Ethical and Regulatory Considerations

Concerns about bias and fairness in decision-making are among the ethical issues raised by the application of AI in finance [10]. Results from models trained on biased data may be discriminatory. Given how sensitive financial data is, data privacy is yet another crucial concern. Institutions must ensure transparency, accountability, and data protection under regulatory frameworks like GDPR and Basel III [5]. The deployment of AI in an ethical manner requires the development of explainable AI models and robust governance frameworks.

6. Results and Discussion

In terms of accuracy and flexibility, AI models typically perform better than conventional techniques. Their intricacy, however, frequently results in difficulties with interpretability, which can impede legal compliance and trust. Faster detection and reaction to fraudulent activities are made possible by real-time processing capabilities, but they also necessitate robust infrastructure and data governance. For financial institutions, the trade-off between model efficacy and transparency is still crucial.

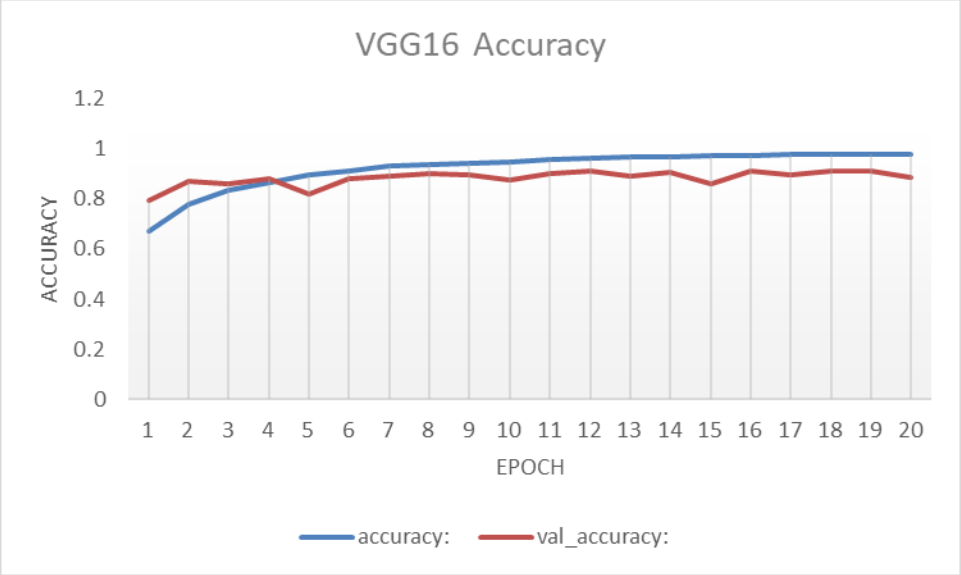

Figure 3:

VGG16 Model Accuracy Results

The VGG16 Model with 20 epochs has been used to train the dataset. This model has a 91% efficacy rate. VGG was used as a feature extractor linked to the dataset in the suggested system. The dataset was divided by the algorithm into 20% validation data and 80% training data. Figure 3's blue line indicates the precision results range of 0.67 to 0.978, while Figure 3's red line indicates the validation precision results range of 0.79 to 0.91.

7. Conclusion

Because AI provides more precise, scalable, and immediate solutions, it has the possibility to completely transform financial risk management and fraud detection. Despite the significant advantages, issues with interpretability, ethics, and regulation need to be resolved. Future research should focus on creating explainable AI models, incorporating federated learning to protect privacy, and investigating hybrid strategies that incorporate several AI modalities.

8. References

[1] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.
[2] Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. European Journal of Operational Research, 247(1), 124-136.
[5] European Commission. (2018). General Data Protection Regulation (GDPR).
[7] Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.
[8] Brown, I., & Mues, C. (2012). An experimental comparison of classification algorithms for imbalanced credit scoring data sets. Expert Systems with Applications, 39(3), 3446-3453.
[9] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58.
[10] Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning. fairmlbook.org.
[11] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.
[12] Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8), 861-874.
[13] Feng, F., He, X., Wang, X., Luo, C., Liu, Y., & Chua, T. S. (2018). Enhancing stock movement prediction with adversarial training. In Proceedings of the 27th ACM International Conference on Information and Knowledge Management (pp. 1249-1258).
[14] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234-245.
[15] Lipton, Z. C. (2018). The mythos of model interpretability. Communications of the ACM, 61(10), 36-43.
[16] Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (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), 559-569.
[17] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network outlier detection techniques. Journal of Network and Computer Applications, 60, 19-31.
[18] T. Jo, Machine Learning Foundations: Supervised, Unsupervised, and Advanced Learning, Springer, 2021

[19] Gandhar, A., Gupta, K., Pandey, A.K. et al. Fraud Detection Using Machine Learning and Deep Learning. SN COMPUT. SCI. 5, 453 (2024). https://doi.org/10.1007/s42979-024-02772-x
[20] JP Morgan, "COiN: Contract Intelligence," 2023. [Online]. Available: https://www.jpmorgan.com
[21] PayPal, "AI in Fraud Detection," 2023. [Online]. Available: https://www.paypal.com
[22] Deutsche Bank, "AI and Google Cloud Partnership," 2023. [Online]. Available: https://www.db.com
[23] SmartDev, "AI for Financial Inclusion," 2023. [Online]. Available: https://www.smartdev.com
[24] Morgan Stanley, "Conversational AI for Advisors," 2023. [Online]. Available: https://www.morganstanley.com
[25] Upstart, "AI Underwriting Platform," 2023. [Online]. Available: https://www.upstart.com
[26] kteppris/fraud-detection-financial-transactions - GitHub
[27] Fraud Detection Dataset - GDPR-Compliant Synthetic Data – Synthesized
[28] M. A. A. Mousa, A. T. Elgohr, and H. Khater, "Path Planning for a 6 DoF Robotic Arm Based on Whale Optimization Algorithm and Genetic Algorithm," Journal of Engineering Research, vol. 7, no. 5, pp. 160-168, 2023, doi: 10.21608/erjeng.2023.237586.1256.
[29] M. Alhamdany and H. Khater, "Proposed Approach for Automatic Underwater Object Classification," ICIC Express Letters, vol. 12, pp. 1205-1212, 2018.
[30] Khater, S. Mesbah, and A. Anwar, "Enhanced navigation system for AUV using mobile application," International Journal of Engineering Inventions, vol. 5, no. 1, pp. 14-19, 2015.
[31] M. A. A. Mousa, A. T. Elgohr, and H. A. Khater, "Trajectory Optimization for a 6 DOF Robotic Arm Based on Reachability Time," Annals of Emerging Technologies in Computing (AETiC), vol. 8, pp. 22-35, 2024.
[32] H. G. Mohamed, H. A. Khater, and K. H. Moussa, "An Intelligent Combined Visual Navigation Brain Model/GPS/MEMS–INS/ADSFCF Method to Develop Vehicle Independent Guidance Solutions," Micromachines, vol. 12, p. 718, 2021, doi: 10.3390/mi12060718.
[33] W. Abdelmoez, H. Khater, and N. El-shoafy, "Comparing maintainability evolution of object-oriented and aspect-oriented software product lines," 2012 8th

International Conference on Informatics and Systems (INFOS), Giza, Egypt, 2012, pp. SE-53-SE-60.
[34] S. S. Saleh, I. Alansari, M. K. Hamiaz, W. Ead, R. A. Tarabishi, and H. Khater, "iFogRep: An intelligent consistent approach for replication and placement of IoT based on fog computing," Egyptian Informatics Journal, vol. 24, no. 2, pp. 327–339, 2023, doi: 10.1016/j.eij.2023.05.003.
[35] Hatem A. Khater, A. Baith Mohamed, Sara M. Kamel,"A proposed technique for software development risks identification by using FTA model," World Academy of Science, Engineering and Technology, IJCIEng., vol. 7, no. 1, pp. 34–40, 2013.
[36] A. A. Farid, G. I. Selim, and H. A. A. Khater, "Applying artificial intelligence techniques to improve clinical diagnosis of Alzheimer's disease," Eur. J. Eng. Science and Technology, vol. 3, no. 2, pp. 58–79, Dec. 2020. doi: 10.33422/ejest.v3i2.487