Artificial Intelligence Techniques for Fraud Detection

Guangsheng Lai *

Posted Date: 15 December 2023

doi: 10.20944/preprints202312.1115.v1

Keywords: Artificial Intelligence; Fraud Detection; Machine Learning; Deep Learning; Supervised learning

Article

Artificial Intelligence Techniques for Fraud Detection

Guangsheng Lai

School of Physics and Information Engineering, Jiangsu Second Normal University, Nanjing, Jiangsu 210016, P R China; 529497288@qq.com

Abstract: In the wake of increasing digital fraud, this paper introduces an innovative application of Artificial Intelligence (AI) in detecting fraudulent activities across finance, healthcare, and e-commerce sectors. It presents a detailed analysis of machine learning methodologies, specifically focusing on the advantages of supervised, unsupervised, and deep learning techniques. The paper addresses the challenges such as data imbalance, model interpretability, and ethical implications in AI-based fraud detection. It also discusses the necessity of high-quality datasets and advocates for the integration of traditional and advanced machine learning methods to enhance accuracy and adaptability in fraud identification. However, it acknowledges the limitations including computational demands and overfitting risks. The study underscores the importance of collaborative efforts between AI experts and industry professionals to develop ethical, efficient, and reliable AI solutions for fraud detection.

Keywords: Artificial Intelligence (AI); Fraud Detection; Machine Learning; Deep Learning; Supervised learning

1. Introduction

Fraud detection, a critical facet in safeguarding various industries, has evolved with the integration of Artificial Intelligence (AI) techniques. The constant threat of fraudulent activities, spanning financial, healthcare, e-commerce[1–3], and other sectors, necessitates sophisticated solutions that go beyond traditional methods. AI, with its capacity to analyze vast datasets, recognize intricate patterns, and identify anomalies, presents a powerful approach to combatting fraud. This intersection of AI and fraud detection not only enhances the speed and accuracy of identifying deceptive practices but also adapts to the evolving nature of fraudulent behaviors across different domains. The introduction of Fraudulent Activities is shown in Figure 1.

Fraud detection encompasses a broad spectrum of deceptive practices, ranging from financial fraud like credit card scams [4,5] and identity theft [6] to industry-specific malfeasance such as insurance[7] and telecommunications fraud[8]. The effectiveness of AI in fraud detection hinges on the diverse array of data sources[9] it can leverage. Transaction records, user profiles, IP addresses, timestamps, and more contribute to the data pool. Real-time processing is paramount, allowing the system to analyze incoming data promptly and respond swiftly to potential threats[10].

At the core of AI-driven fraud detection are various machine learning techniques tailored to different needs[11,12]. Supervised learning[13] utilizes labeled data to train models on known instances of fraud and non-fraud, enabling predictions on new data. Unsupervised learning, on the other hand, identifies patterns and anomalies without labeled data[14,15], often employing clustering and outlier detection methods[16,17]. Feature engineering, a crucial step in the process, involves selecting and transforming relevant features from the data[18]. This strategic manipulation enhances the model's ability to detect fraud by aggregating transaction data, creating new variables, and normalizing existing ones.

Anomaly detection, a pivotal aspect of AI-powered fraud detection[19], involves the identification of unusual patterns or outliers that may signify fraudulent activity. Employing statistical methods, clustering algorithms, and machine learning models, anomaly detection adds a layer of sophistication to the system's capabilities. Behavioral analysis, another integral component,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2023 doi:10.20944/preprints202312.1115.v1

assesses historical user or entity behavior to identify deviations from normal patterns. By establishing baselines for regular behavior, the system can efficiently flag activities falling outside these norms[20]. Operating in real-time or near real-time, fraud detection systems ensure a swift response to potential threats, showcasing the dynamic and proactive nature of AI in combating fraudulent activities across diverse industries[21].

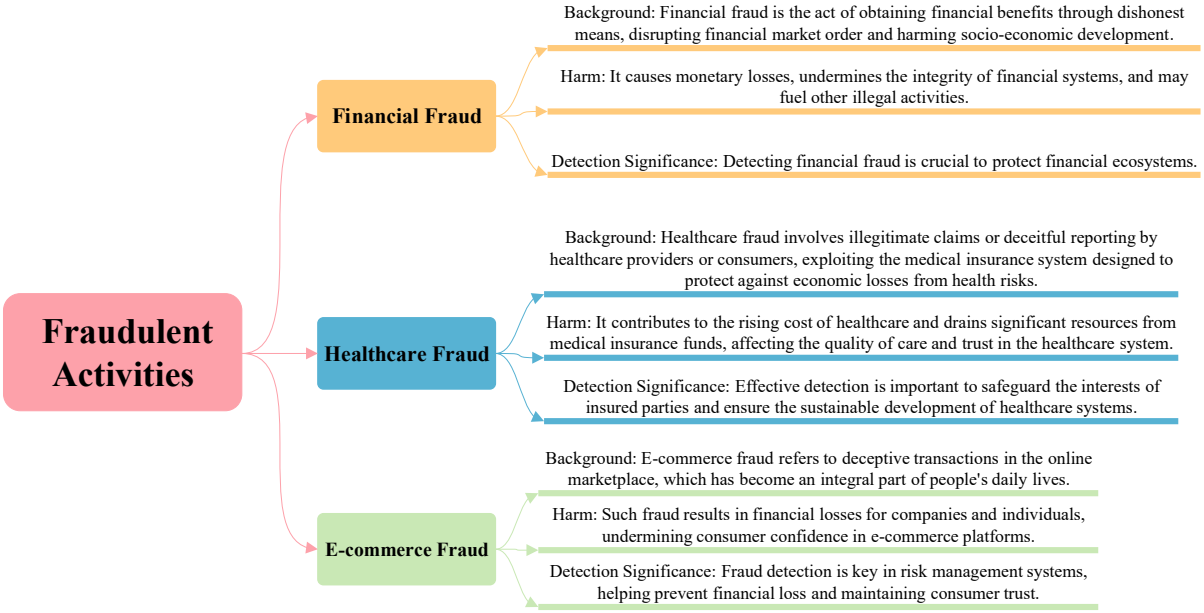

Figure 1. The introduction of Fraudulent Activities.

2. Machine Learning

Machine Learning (ML) [22] is a subset of artificial intelligence (AI) that empowers computers to learn from data and improve their performance without being explicitly programmed. The primary objective of machine learning is to enable systems to recognize patterns, make decisions [23], and improve their performance over time based on experience. Unlike traditional rule-based programming, where explicit instructions are provided to accomplish a task, machine learning algorithms use data to iteratively refine their models, allowing them to adapt and generalize to new situations[24,25].

There are several types of machine learning, each serving distinct purposes. The comparison of different machine learning is shown in Table 1. Supervised learning involves training a model on a labeled dataset, where the algorithm learns to map input data to corresponding output labels[26]. Unsupervised learning, in contrast, deals with unlabeled data, aiming to discover patterns and structures within the information. Reinforcement learning involves an agent learning by interacting with an environment and receiving feedback in the form of rewards or penalties, allowing it to optimize its behavior over time. These diverse approaches cater to different applications, from predicting outcomes to clustering data and even training agents for autonomous decision-making[27].

Table 1. The comparison of different machine learning.

Dataset	Core Formula	Characteristic	Limitations
Bayesian Classification	$f(x) = \arg\max_{c \in C} P(c \mid x)$	Supports incremental training, assumes feature independence.	Unable to handle feature combinations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2023 doi:10.20944/preprints202312.1115.v1

Logistic Regression	$f(x) = sign(\sum_i \omega_i x_i + b)$	Easy to model, supports incremental training.	Outlier sensitivity.
Support Vector Machine	$f(x) = \omega^T x + b$ $s.t. yf(x) \geq 1$	Strong robustness, can be nonlinear mapping.	Difficult to implement large-scale training.
Decision Trees	$Info(D) = -\sum_i p_i \log p_i$	Clear rules, can handle outliers.	Data-dependent, easy to overfitting.
k-Nearest Neighbor	$f(x) = \arg\max_{x_i \in N_k(x)} I(y_i = c_j),$ $i = 1, 2, \cdots, N; j = 1, 2, \cdots, k;$	Supports incremental training, robust to missing values, parameter independence and noise.	Slow classification speed, high cost of large-scale computation.
Ensemble Learning	$H(x) = sign(\sum_i h_i(x))$	Strong robustness and high accuracy.	Increase computational cost, poor parallelism of some algorithms.
Neural Network	$f(x) = \sigma(\sum_i \omega_i x_i + b_i)$	Autonomous learning, can be nonlinear fitting.	Unable to fit complex functions, poor interpretability.
Deep Learning	$f(x) = \sigma(\sum_i \omega_i x_i + b_i)$	Strong learning ability, high accuracy.	The computational and annotation costs are high, and some hyperparameters need to be determined empirically.

The versatility of machine learning is reflected in its wide range of applications across various industries. In healthcare, machine learning is employed for disease diagnosis, personalized treatment plans, and drug discovery[28]. In finance, algorithms are used for fraud detection, risk assessment, and algorithmic trading[29]. Marketing benefits from machine learning through customer segmentation, personalized recommendations, and predictive analytics[30]. In natural language processing (NLP), machine learning enables sentiment analysis, language translation, and chatbot interactions[31]. These applications showcase the adaptability of machine learning in solving complex problems and making data-driven decisions.

While machine learning has achieved significant successes, it is not without challenges. Issues such as bias in algorithms, interpretability of models, and the need for large labeled datasets pose ongoing concerns. The future of machine learning involves addressing these challenges, exploring more advanced techniques like deep learning, and pushing the boundaries of what AI systems can achieve. As machine learning continues to evolve, its integration with other emerging technologies, such as quantum computing[32] and explainable AI[33], holds promise for overcoming existing limitations and unlocking new possibilities for solving complex problems in diverse fields.

3. Traditional ML Approaches to Fraud Detection

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2023 doi:10.20944/preprints202312.1115.v1

Traditional machine learning (ML) [34,35] approaches have played a pivotal role in the realm of fraud detection, providing effective means to analyze and interpret data patterns indicative of fraudulent activities. These methods leverage supervised learning techniques, where algorithms are trained on historical data labeled with instances of fraud and non-fraud. The primary goal is to enable the system to generalize from past examples, learning to distinguish between normal and anomalous behavior in new data.

Supervised learning forms the cornerstone of traditional ML approaches to fraud detection[36]. During the training phase, the algorithm learns from a labeled dataset, identifying patterns and features associated with known instances of fraud. This knowledge is then applied to new, unlabeled data to predict whether a particular transaction or activity is likely to be fraudulent. Common supervised learning algorithms in fraud detection include decision trees[37], logistic regression[38], and support vector machines[39]. For example, the structure diagram of the decision tree is shown in Figure 2. The effectiveness of these models relies on the quality and representativeness of the training data.

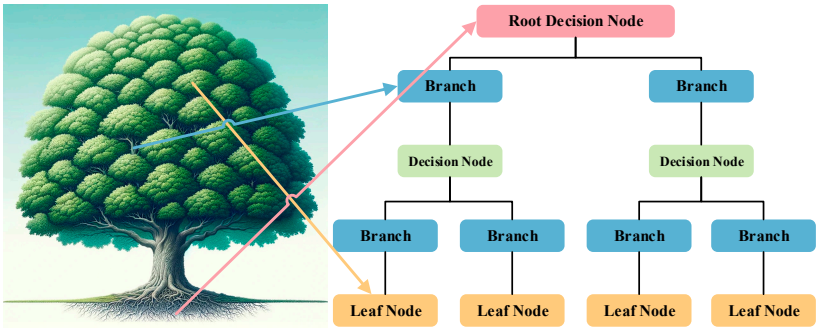

Figure 2. The structure diagram of the decision tree.

In addition to supervised learning, traditional ML approaches [40,41] often incorporate unsupervised learning techniques, particularly for anomaly detection. Anomalous behavior in data, which may signify fraudulent activity, is identified without the use of labeled examples. Clustering algorithms, such as k-means[42], and density-based methods, like isolation forests[43], are commonly employed to detect outliers or patterns that deviate from the norm. Unsupervised learning is valuable in scenarios where labeled fraud data is scarce, providing a complementary approach to supervised methods[44].

Feature engineering is a critical aspect of traditional ML approaches in fraud detection. The selection and transformation of relevant features from the data enhance the model's ability to discern fraudulent patterns. Feature engineering may involve creating new variables, aggregating transaction data, or normalizing existing features. Furthermore, the interpretability of models is essential for understanding the rationale behind fraud predictions. Transparent models, such as decision trees[45], offer insights into the features contributing to a prediction, aiding analysts in comprehending and validating the model's decisions.

Despite their effectiveness, traditional ML approaches for fraud detection have limitations. They may struggle to adapt to rapidly evolving fraud tactics and may be less effective in handling highly imbalanced datasets. As fraudsters continuously refine their techniques, there is a growing need for more advanced and adaptive methods. The future of fraud detection lies in the integration of traditional approaches with emerging technologies, such as deep learning and ensemble methods, to enhance accuracy and robustness. Additionally, addressing challenges like model interpretability and ethical considerations[46,47] remains a focal point for refining and advancing traditional ML techniques in the context of fraud detection.

4. Deep Learning Approaches to Fraud Detection

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2023 doi:10.20944/preprints202312.1115.v1

Deep Learning has emerged as a potent tool in the realm of fraud detection, leveraging complex neural networks to automatically learn and extract intricate patterns within large datasets[48]. In contrast to traditional machine learning methods, deep learning approaches delve into multiple layers of abstraction [49,50], enabling the automatic discovery of features and representations that may be challenging to capture using manual feature engineering. This adaptability is particularly advantageous in the context of fraud detection, where fraudulent patterns can be dynamic and non-linear[51].

Deep learning models applied to fraud detection often involve architectures such as deep neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and more recently, transformer-based models. Deep neural networks are adept at learning hierarchical representations of features from transactional and user behavior data[52]. CNNs are effective for spatial data, such as images associated with fraud detection[53], while RNNs are valuable for capturing temporal dependencies in sequential data[54]. Transformer models, originally developed for natural language processing, have shown promise in capturing long-range dependencies and contextual information relevant to fraud detection[55,56].

The Transformer model consists of two main parts, the Encoder and the Decoder. The model of the Transformer is shown in Figure 3. The left part is the encoder which is composed of multiple layers of attention mechanisms and feed-forward neural networks and follows the residual normalization process, where the output of each layer is a multidimensional vector, and the output vector of each layer is the input of the next layer. On the right is the decoder, which also has the two layers of the encoder, but between them there is an Encoder-Decoder Attention, which is used to help the decoder to focus on the relevant parts of the input sentence[57].

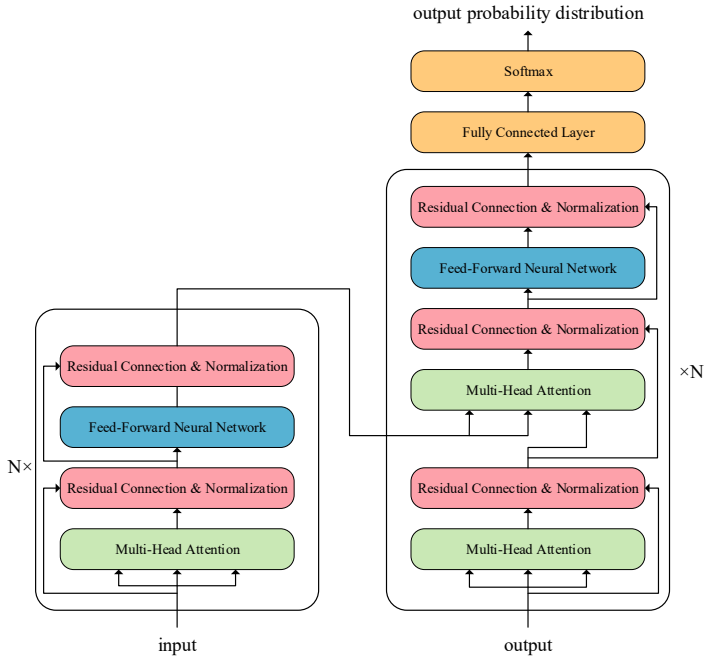

Figure 3. Transformer Model Diagram.

Training deep learning models [58] for fraud detection requires substantial amounts of labeled data, which can be a challenge due to the imbalance between normal and fraudulent instances[59]. Data preprocessing techniques, including resampling, oversampling, and undersampling, are employed to address this imbalance [60]. Additionally, transfer learning, where a model pre-trained on a large dataset is fine-tuned for fraud detection, can enhance performance[61]. Training strategies also involve the use of autoencoders for unsupervised feature learning and anomaly detection[62], enabling the model to identify patterns indicative of fraud without explicit labels.

Despite their success, deep learning approaches to fraud detection face challenges, including interpretability and explainability[63,64]. The inherent complexity of deep neural networks can make

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2023 doi:10.20944/preprints202312.1115.v1

it challenging to understand the reasoning behind specific predictions, raising concerns about the transparency of decision-making processes. Ethical considerations, such as bias in algorithms and the potential for discriminatory outcomes, are also critical concerns that researchers and practitioners in the field are actively addressing to ensure fair and unbiased fraud detection.

The future of deep learning in fraud detection involves addressing current challenges and integrating with traditional machine learning approaches. Hybrid models that combine the strengths of deep learning and traditional methods are being explored to enhance robustness and interpretability[65]. Further advancements in explainable AI[66], regularization techniques[67], and the development of more efficient training strategies are anticipated to propel deep learning approaches to the forefront of fraud detection, contributing to the ongoing efforts to mitigate evolving threats and protect against fraudulent activities in diverse domains.

5. Common Fraud Detection Datasets

High-quality datasets play a crucial role in the development, training, and evaluation of fraud detection models. They serve as the foundation for teaching algorithms to distinguish between legitimate and fraudulent patterns within the data. Common fraud detection datasets provide researchers and practitioners with representative samples of real-world scenarios, enabling them to build robust models that can generalize well to diverse and evolving fraud patterns[68].

Several widely used datasets are instrumental in advancing research and development in fraud detection. The Credit Card Fraud Detection dataset, available on platforms like Kaggle, comprises anonymized credit card transactions, with a significant class imbalance between normal and fraudulent instances[69]. The IEEE-CIS Fraud Detection dataset, introduced by the Institute of Electrical and Electronics Engineers (IEEE), focuses on e-commerce transactions, offering a diverse set of features for comprehensive model training , the composition of the data set is shown in Figure 4. Another notable dataset is the Synthetic Financial Datasets for Fraud Detection, which provides synthetic but realistic financial data for assessing the performance of fraud detection algorithms.

Figure 4. The composition of the data set.

Common fraud detection datasets share certain characteristics essential for the effectiveness of machine learning models. Imbalanced class distribution, where the majority of instances are non-fraudulent, mirrors the real-world scenario but necessitates careful handling to prevent model bias[70]. Temporal aspects, such as time-based patterns in transaction data, are often present to capture the dynamic nature of fraudulent activities. Datasets may also include features like

 doi:10.20944/preprints202312.1115.v1

transaction amounts, timestamps, and user behavior, providing a holistic representation of the factors contributing to fraud.

While common fraud detection datasets offer valuable resources, challenges persist. The rapidly evolving nature of fraud necessitates continuous updates and expansions of datasets to reflect emerging patterns and tactics employed by fraudsters. Furthermore, ensuring the privacy and security of sensitive information within datasets is of paramount importance, prompting the development of synthetic datasets that mimic real-world characteristics without compromising individual privacy[71]. The collaborative efforts of the research community, industry, and regulatory bodies are crucial for addressing these challenges and maintaining the relevance of common fraud detection datasets in the ongoing pursuit of effective fraud prevention and detection strategies.

6. Conclusion

In conclusion, the integration of AI techniques into fraud detection has marked a transformative leap in the ability to combat deceptive practices across various industries. The dynamic and adaptive nature of AI enables the analysis of vast datasets, the identification of intricate patterns, and the detection of anomalies that may signify fraudulent activities. From machine learning algorithms, including supervised and unsupervised learning, to advanced deep learning architectures like neural networks, AI methods provide a comprehensive toolkit for discerning fraudulent patterns in diverse data sources.

The significance of AI in fraud detection is evident in its applications across sectors such as finance, healthcare, e-commerce, and beyond. Through personalized medicine, predictive analytics, and real-time transaction monitoring, AI contributes to the proactive identification and prevention of fraudulent behaviors. The adaptability of machine learning models allows for continuous learning and adjustment to evolving fraud tactics, making these techniques indispensable in the ongoing battle against fraudsters.

Common challenges, including the need for labeled datasets, model interpretability, and ethical considerations, underscore the importance of ongoing research and development in the field. As technology progresses, the integration of traditional and deep learning approaches, along with advancements in explainable AI and ethical considerations, is shaping the future landscape of fraud detection. Collaborative efforts between researchers, industry experts, and regulatory bodies are essential to address emerging challenges, ensure data privacy, and foster the responsible and effective use of AI techniques in the pursuit of securing financial transactions, sensitive information, and the integrity of various systems against fraudulent activities[72]. The continued refinement of artificial intelligence for fraud detection not only safeguards businesses and individuals but also reflects the collective commitment to staying one step ahead in the ever-evolving landscape of digital security.

Funding: The research work was supported by the open project of State Key Laboratory of Millimeter Waves (Grant No. K202218)

Data Availability Statement: There is no data associated with this paper.

Acknowledgment: We thank all the anonymous reviewers for their hard reviewing work.

Conflict of Interest: The author declares there is no conflict of interest regarding this paper.

References

1. Y. Y. Festa and I. A. Vorobyev, "A hybrid machine learning framework for e-commerce fraud detection," *Model Assisted Statistics and Applications,* vol. 17, pp. 41-49, 2022.
2. N. Kumaraswamy, T. Ekin, C. Park, M. K. Markey, J. C. Barner, and K. Rascati, "Using a Bayesian Belief Network to detect healthcare fraud," *Expert Systems with Applications,* vol. 238, 2024.
3. G. Tong and J. Shen, "Financial transaction fraud detector based on imbalance learning and graph neural network," *Applied Soft Computing,* vol. 149, 2023.

4. Y. Bing Chu, Z. Min Lim, B. Keane, P. Hao Kong, A. Rafat Elkilany, and O. Hisham Abusetta, "Credit Card Fraud Detection on Original European Credit Card Holder Dataset Using Ensemble Machine Learning Technique," *Journal of Cyber Security,* vol. 5, pp. 33-46, 2023.
5. Y. Fang, Y. Zhang, and C. Huang, "Credit Card Fraud Detection Based on Machine Learning," *Computers, Materials & Continua,* vol. 61, pp. 185-195, 2019.
6. S. Vaithyasubramanian, D. Saravanan, and C. K. Kirubhashankar, "Communal Fraud Detection Algorithm for Establishing Identity Thefts in Online Shopping," *International Journal of e-Collaboration,* vol. 17, pp. 75-84, 2021.
7. S. Xiao, T. Bai, X. Cui, B. Wu, X. Meng, and B. Wang, "A graph-based contrastive learning framework for medicare insurance fraud detection," *Frontiers of Computer Science,* vol. 17, 2023.
8. X. Hu, H. Chen, S. Liu, H. Jiang, G. Chu, and R. Li, "BTG: A Bridge to Graph machine learning in telecommunications fraud detection," *Future Generation Computer Systems,* vol. 137, pp. 274-287, 2022.
9. M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions," *IEEE/CAA Journal of Automatica Sinica,* vol. 9, pp. 407-436, 2022.
10. A. K. Junejo, M. Breza, and J. A. McCann, "Threat Modeling for Communication Security of IoT-Enabled Digital Logistics," *Sensors (Basel),* vol. 23, 2023.
11. M. Abdalsalam, C. Li, A. Dahou, and N. Kryvinska, "Terrorism Attack Classification Using Machine Learning: The Effectiveness of Using Textual Features Extracted from GTD Dataset," *Computer Modeling in Engineering & Sciences,* vol. 138, pp. 1427-1467, 2024.
12. J. T. Hancock, R. A. Bauder, H. Wang, and T. M. Khoshgoftaar, "Explainable machine learning models for Medicare fraud detection," *Journal of Big Data,* vol. 10, 2023.
13. S. Subudhi and S. Panigrahi, "Two-Stage Automobile Insurance Fraud Detection by Using Optimized Fuzzy C-Means Clustering and Supervised Learning," *International Journal of Information Security and Privacy,* vol. 14, pp. 18-37, 2020.
14. J. Debener, V. Heinke, and J. Kriebel, "Detecting insurance fraud using supervised and unsupervised machine learning," *Journal of Risk and Insurance,* vol. 90, pp. 743-768, 2023.
15. F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," *Information Sciences,* vol. 557, pp. 317-331, 2021.
16. "WXGCB: A Clustering Prior Weighting Semi-Supervised Learning Method Based on Space Level Constraint and Mixed Variable Metrics," *Advances in Computer, Signals and Systems,* vol. 7, 2023.
17. Y. Huang, W. Liu, S. Li, Y. Guo, and W. Chen, "A Novel Unsupervised Outlier Detection Algorithm Based on Mutual Information and Reduced Spectral Clustering," *Electronics,* vol. 12, 2023.
18. N. Kumaraswamy, M. K. Markey, J. C. Barner, and K. Rascati, "Feature engineering to detect fraud using healthcare claims data," *Expert Systems with Applications,* vol. 210, 2022.
19. A. J. Mary and S. P. A. Claret, "Design and development of big data-based model for detecting fraud in healthcare insurance industry," *Soft Computing,* vol. 27, pp. 8357-8369, 2023.
20. J. Li and D. Yang, "Research on Financial Fraud Detection Models Integrating Multiple Relational Graphs," *Systems,* vol. 11, 2023.
21. I. Kose, M. Gokturk, and K. Kilic, "An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance," *Applied Soft Computing,* vol. 36, pp. 283-299, 2015.
22. Y. Zhang, "Preliminary research on abnormal brain detection by wavelet-energy and quantum-behaved PSO," *Technology and Health Care,* vol. 24, pp. S641-S649, 2016.

23. S.-H. Wang, "Multiple Sclerosis Identification Based on Fractional Fourier Entropy and a Modified Jaya Algorithm," *Entropy,* vol. 20, p. 254, 2018.
24. W. T. Kerr and K. N. McFarlane, "Machine Learning and Artificial Intelligence Applications to Epilepsy: a Review for the Practicing Epileptologist," *Curr Neurol Neurosci Rep*, 2023.
25. S. Salman, Q. Gu, R. Sharma, Y. Wei, B. Dherin, S. Reddy, *et al.*, "Artificial intelligence and machine learning in aneurysmal subarachnoid hemorrhage: Future promises, perils, and practicalities," *J Neurol Sci,* vol. 454, p. 120832, 2023.
26. H. Dai, G. Cai, Z. Lin, Z. Wang, and Q. Ye, "Validation of Inertial Sensing-Based Wearable Device for Tremor and Bradykinesia Quantification," *IEEE J Biomed Health Inform,* vol. 25, pp. 997-1005, 2021.
27. H. Sibyan, W. Suharso, E. Suharto, M. A. Manuhutu, and A. P. Windarto, "Optimization of Unsupervised Learning in Machine Learning," *Journal of Physics: Conference Series,* vol. 1783, 2021.
28. S. Geoffrion, C. Morse, M. M. Dufour, N. Bergeron, S. Guay, and M. J. Lanovaz, "Screening for Psychological Distress in Healthcare Workers Using Machine Learning: A Proof of Concept," *J Med Syst,* vol. 47, p. 120, 2023.
29. X. Zhang, X. Ai, X. Wang, G. Zong, and J. Zhang, "A Study on the Effects of Digital Finance on Green Low-Carbon Circular Development Based on Machine Learning Models," *Mathematics,* vol. 11, 2023.
30. L. J. Paas, "Marketing analytics stages: Demystifying and deploying machine learning," *International Journal of Market Research,* vol. 65, pp. 687-707, 2023.
31. A. Pattison, W. Cipolli, J. Marichal, and C. Cherniakov, "Fracking Twitter: Utilizing machine learning and natural language processing tools for identifying coalition and causal narratives," *Politics & Policy,* vol. 51, pp. 755-774, 2023.
32. G. Balamurugan, C. Annadurai, I. Nelson, K. Nirmala Devi, A. S. Oliver, and S. Gomathi, "Optical bio sensor based cancer cell detection using optimized machine learning model with quantum computing," *Optical and Quantum Electronics,* vol. 56, 2023.
33. L. Malandri, F. Mercorio, M. Mezzanzanica, and A. Seveso, "Model-contrastive explanations through symbolic reasoning," *Decision Support Systems,* vol. 176, 2024.
34. Y. Zhang, "Pathological brain detection in MRI scanning via Hu moment invariants and machine learning," *Journal of Experimental & Theoretical Artificial Intelligence,* vol. 29, pp. 299-312, 2017.
35. Y. Zhang, "Pathological brain detection in MRI scanning by wavelet packet Tsallis entropy and fuzzy support vector machine," *SpringerPlus,* vol. 4, Article ID: 716, 2015.
36. S. Yang, P. Varghese, E. Stephenson, K. Tu, and J. Gronsbell, "Machine learning approaches for electronic health records phenotyping: a methodical review," *J Am Med Inform Assoc,* vol. 30, pp. 367-381, 2023.
37. D. C. Gkikas, P. K. Theodoridis, T. Theodoridis, and M. C. Gkikas, "Finding Good Attribute Subsets for Improved Decision Trees Using a Genetic Algorithm Wrapper; a Supervised Learning Application in the Food Business Sector for Wine Type Classification," *Informatics,* vol. 10, 2023.
38. K. Vo, J. Jonnagaddala, and S. T. Liaw, "Statistical supervised meta-ensemble algorithm for medical record linkage," *J Biomed Inform,* vol. 95, p. 103220, 2019.
39. A. Mignan, "A preliminary text classification of the precursory accelerating seismicity corpus: inference on some theoretical trends in earthquake predictability research from 1988 to 2018," *Journal of Seismology,* vol. 23, pp. 771-785, 2019.
40. L. N. Wu, "Pattern Recognition via PCNN and Tsallis Entropy," *Sensors,* vol. 8, pp. 7518-7529, 2008.
41. Y. Zhang, "Color Image Enhancement based on HVS and PCNN," *SCIENCE CHINA Information Sciences,* vol. 53, pp. 1963-1976, 2010.

42. O. Iparraguirre-Villanueva, V. Guevara-Ponce, F. Sierra-Linan, S. Beltozar-Clemente, and M. Cabanillas-Carbonell, "Sentiment Analysis of Tweets using Unsupervised Learning Techniques and the K-Means Algorithm," *International Journal of Advanced Computer Science and Applications,* vol. 13, 2022.
43. T. Barbariol and G. A. Susto, "TiWS-iForest: Isolation forest in weakly supervised and tiny ML scenarios," *Information Sciences,* vol. 610, pp. 126-143, 2022.
44. S. Lin, G. Mengaldo, and R. Maulik, "Online data-driven changepoint detection for high-dimensional dynamical systems," *Chaos,* vol. 33, 2023.
45. Y. Wang, Y. Liu, J. Zhao, and Q. Zhang, "A Low-Complexity Fast CU Partitioning Decision Method Based on Texture Features and Decision Trees," *Electronics,* vol. 12, 2023.
46. X. Li, M. Sale, K. Nieforth, K. L. Bigos, J. Craig, F. Wang, *et al.*, "pyDarwin: A Machine Learning Enhanced Automated Nonlinear Mixed-effect Model Selection Toolbox," *Clin Pharmacol Ther*, 2023.
47. M. El Hajj and J. Hammoud, "Unveiling the Influence of Artificial Intelligence and Machine Learning on Financial Markets: A Comprehensive Analysis of AI Applications in Trading, Risk Management, and Financial Operations," *Journal of Risk and Financial Management,* vol. 16, 2023.
48. M. Maashi, B. Alabduallah, and F. Kouki, "Sustainable Financial Fraud Detection Using Garra Rufa Fish Optimization Algorithm with Ensemble Deep Learning," *Sustainability,* vol. 15, 2023.
49. S.-H. Wang and S. Fernandes, "AVNC: Attention-based VGG-style network for COVID-19 diagnosis by CBAM," *IEEE Sensors Journal,* vol. 22, pp. 17431 - 17438, 2022.
50. Y.-D. Zhang, "MIDCAN: A multiple input deep convolutional attention network for Covid-19 diagnosis based on chest CT and chest X-ray," *Pattern Recognition Letters,* vol. 150, pp. 8-16, 2021.
51. Z. Li, M. Huang, G. Liu, and C. Jiang, "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection," *Expert Systems with Applications,* vol. 175, 2021.
52. T. Barcin, M. A. Yucel, R. H. Ersan, M. A. Alagoz, A. Dogen, S. Burmaoglu, *et al.*, "Deep learning approach to the discovery of novel bisbenzazole derivatives for antimicrobial effect," *Journal of Molecular Structure,* vol. 1295, 2024.
53. X. Wu, S. Jiang, G. Li, S. Liu, B. Metcalfe, L. Chen, *et al.*, "Deep Learning With Convolutional Neural Networks for Motor Brain-Computer Interfaces Based on Stereo-Electroencephalography (SEEG)," *IEEE J Biomed Health Inform,* vol. 27, pp. 2387-2398, 2023.
54. M. R. Sarkar, S. G. Anavatti, T. Dam, M. M. Ferdaus, M. Tahtali, S. Ramasamy, *et al.*, "GATE: A guided approach for time series ensemble forecasting," *Expert Systems with Applications,* vol. 235, 2024.
55. Y. Li, J. Cao, Y. Xu, L. Zhu, and Z. Y. Dong, "Deep learning based on Transformer architecture for power system short-term voltage stability assessment with class imbalance," *Renewable and Sustainable Energy Reviews,* vol. 189, 2024.
56. G. B. Kim, J. Y. Kim, J. A. Lee, C. J. Norsigian, B. O. Palsson, and S. Y. Lee, "Functional annotation of enzyme-encoding genes using deep learning with transformer layers," *Nat Commun,* vol. 14, p. 7370, 2023.
57. L. Wang, M. Ye, Y. Lu, Q. Qiu, Z. Niu, H. Shi, *et al.*, "A combined encoder-transformer-decoder network for volumetric segmentation of adrenal tumors," *Biomed Eng Online,* vol. 22, p. 106, 2023.
58. Y. Zhang, "Deep learning in food category recognition," *Information Fusion,* vol. 98, p. 101859, 2023.
59. Z. S. Rubaidi, B. B. Ammar, and M. B. Aouicha, "Fraud Detection Using Large-scale Imbalance Dataset," *International Journal on Artificial Intelligence Tools,* vol. 31, 2022.
60. X.-X. Hou, "Voxelwise detection of cerebral microbleed in CADASIL patients by leaky rectified linear unit and early stopping," *Multimedia Tools and Applications,* vol. 77, pp. 21825-21845, 2018.

61. D. Sisodia and D. S. Sisodia, "A transfer learning framework towards identifying behavioral changes of fraudulent publishers in pay-per-click model of online advertising for click fraud detection," *Expert Systems with Applications,* vol. 232, 2023.
62. J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, "On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders," *Applied Sciences,* vol. 12, 2022.
63. Y. Gao, J. Liu, W. Li, M. Hou, Y. Li, and H. Zhao, "Augmented Grad-CAM++: Super-Resolution Saliency Maps for Visual Interpretation of Deep Neural Network," *Electronics,* vol. 12, 2023.
64. D. Probst, "An explainability framework for deep learning on chemical reactions exemplified by enzyme-catalysed reaction classification," *J Cheminform,* vol. 15, p. 113, 2023.
65. E. Kim, J. Lee, H. Shin, H. Yang, S. Cho, S.-k. Nam, *et al.*, "Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning," *Expert Systems with Applications,* vol. 128, pp. 214-224, 2019.
66. W. van Zetten, G. J. Ramackers, and H. H. Hoos, "Increasing trust and fairness in machine learning applications within the mortgage industry," *Machine Learning with Applications,* vol. 10, 2022.
67. Y. Liu, "Design of XGBoost prediction model for financial operation fraud of listed companies," *International Journal of System Assurance Engineering and Management,* vol. 14, pp. 2354-2364, 2023.
68. B. Xu, Y. Wang, X. Liao, and K. Wang, "Efficient fraud detection using deep boosting decision trees," *Decision Support Systems,* vol. 175, 2023.
69. A. Alharbi, M. Alshammari, O. D. Okon, A. Alabrah, H. T. Rauf, H. Alyami, *et al.*, "A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach," *Electronics,* vol. 11, 2022.
70. A. G. Sharifai and Z. B. Zainol, "Multiple Filter-Based Rankers to Guide Hybrid Grasshopper Optimization Algorithm and Simulated Annealing for Feature Selection With High Dimensional Multi-Class Imbalanced Datasets," *IEEE Access,* vol. 9, pp. 74127-74142, 2021.
71. J. Chen, Q. Chen, F. Jiang, X. Guo, K. Sha, and Y. Wang, "SCN_GNN: A GNN-based fraud detection algorithm combining strong node and graph topology information," *Expert Systems with Applications,* vol. 237, 2024.
72. R. Ramesh, R. Dodmane, S. Shetty, G. Aithal, M. Sahu, and A. Sahu, "A Novel and Secure Fake-Modulus Based Rabin-3 Cryptosystem," *Cryptography,* vol. 7, 2023.