

Artificial Intelligence and Fraud Detection: An Overview

Wuku Astuti¹, Bhenu Artha^{2*}, Atha Raihan³, Sarimutiara Tumanggor⁴
wukuastuti@gmail.com¹, bhenoz27@gmail.com^{2*}
^{1,2,3,4}Universitas Widya Mataram, Yogyakarta

Article History

Received: 15 June 2025
Accepted: 19 August 2025
Publish : 16 Sept 2025

Keywords: Artificial
Intelligence, Fraud,
Technology, Development

Abstract

The digital revolution, unquestionably, has changed nations by promoting greater connectivity and quickening development. The digital revolution is giving nations the means to close infrastructure gaps, take advantage of international opportunities, and promote sustainable growth in a variety of industries, from e-commerce and digital banking. At this critical point, a paradigm shift is needed to develop a new artificial intelligence (AI)-powered line of defense. One of the most important uses of artificial intelligence in the finance industry is fraud detection. The way financial institutions, companies, and organizations detect and stop fraudulent activity has completely changed because of the combination of cutting-edge AI technologies with complex detection methods. The present status, approaches, difficulties, and potential future paths of AI-driven fraud detection systems are all examined in this thorough analysis. A theoretical literature review is conducted to achieve the research's goals and objectives, and a conceptual framework for future study is offered. In the current research, authors consider fraud detection as dependent variable affected by AI. AI-driven systems have proven remarkably successful in detecting fraudulent activity while reducing false positives, from deep learning architectures that capture intricate temporal and spatial patterns to machine learning algorithms that get better over time. AI's involvement in protecting financial systems and lowering losses is growing as financial fraud grows more complex.

Introduction

The digital revolution, unquestionably, has changed nations by promoting greater connectivity and quickening development. The digital revolution is giving nations the means to close infrastructure gaps, take advantage of international opportunities, and promote sustainable growth in a variety of industries, from e-commerce and digital banking (Odufisan et al., 2025). At this critical point, a paradigm shift is needed to develop a new artificial intelligence (AI)-powered line of defense.

The ability of robots to mimic human intelligence in behavior is known as artificial intelligence, and it is achieved by studying how the human brain learns, makes decisions, and solves problems (Abhulimen & Erastus, 2022). AI seeks to imitate these qualities in robots so they can carry out tasks like thinking, language comprehension, pattern recognition, and input adaptation that normally need human intellect. AI is powered by techniques that allow robots to operate intelligently, even in complicated or uncertain situations. It can take many different forms, such as expert systems, speech recognition software, and sophisticated robotics (Odufisan et al., 2025).

One of the most important uses of artificial intelligence in the finance industry is fraud detection. The way financial institutions, companies, and organizations detect and stop fraudulent activity has completely changed because of the combination of cutting-edge AI technologies with complex detection methods. The present status, approaches, difficulties, and potential future paths of AI-driven fraud detection systems are all examined in this thorough analysis. The goal of artificial intelligence (AI), a relatively new technology, is to improve human intelligence or work capacity. It has a wide range of applications (Ahmad et al., 2021, 2022; Kolotylo-Kulkarni et al., 2021). AI is a technical term that

uses intellectual stimulation and development to assess and actualize a human's normal brain processes (Ahmad et al., 2022). Algorithms that replicate human mental processes form the basis of AI technology. Through a variety of applications that advance society, AI combines social science and engineering. It can recognize human commands and use algorithms to evaluate data in a manner akin to that of human minds.

AI has seen a rise in commercial applications due to the development of modern science and technology, which has altered the way people live and work. It has several advantages, especially in e-commerce, and is becoming more of its motivator (Helmy Mohamad et al., 2022). AI is gaining traction in both academia and business, attracting scholars to improve its technological developments and broaden its applications in a variety of fields. These days, it helps people perform a variety of tasks, etc. Consequently, it is one of the primary sources of the current era of development (Ran et al., 2020).

Organizations have historically used a combination of pre-established procedures and manual fraud detection analysis to protect their operations and clients, although these techniques have been useful in the past, they are becoming less effective in the face of constantly changing dangers (Odufisan et al., 2025). One of the main issues with conventional fraud detection methods is their lack of flexibility (Olufemi et al., 2024). These systems typically operate using a predefined set of rules that identify behaviors that either meet or exceed certain criteria. These laws may have been effective in the past, but they can't keep up with the evolving nature of fraud. Fraudsters are constantly developing new concepts and tactics to get past these recognized red flags. Updating these rule-based systems to address new risks is sometimes a laborious and slow process (Liu et al., 2021). Fraudsters have an opportunity to exploit a gap in the detection criteria that permits the introduction of new fraud tactics (Hernandez Aros et al., 2024; Su et al., 2025). By dividing a large purchase into multiple smaller transactions, each of which falls below the threshold and avoids detection, a fraudster might easily circumvent an e-commerce platform regulation that marks transactions over a specific amount as potentially fraudulent (Odufisan et al., 2025).

The lack of sophistication in pattern identification is another issue with traditional approaches. Complex connections and relationships between various data pieces may be a part of fraudulent operations (Hilal et al., 2022). A few instances of the distinct elements of a fraudulent transaction include the use of a new user account, a billing address that differs from the shipping address, and an effort to purchase a remote location. These subtle but important patterns may be missed by hand analysis or rule-based algorithms that concentrate only on individual data items. Lastly, there are serious scaling issues with conventional approaches. The digital age is marked by an explosion of data (Theodorakopoulos et al., 2024). The volume of user interactions, online transactions, and data points is continuously increasing, making human analysis of this data increasingly difficult and time-consuming. These massive datasets may be too big for traditional approaches to handle (Odufisan et al., 2025). This could lead to an accumulation of unprocessed data, creating opportunities for fraudulent activities to avoid discovery. Even if conventional fraud detection techniques have historically helped protect businesses, their shortcomings are becoming more obvious in the fast-paced digital environment of today. Fraudsters can take advantage of these vulnerabilities because of their incapacity to handle massive datasets, recognize intricate patterns, and adjust to changing threats (Amos Kipngetich, 2025; U. Bansal et al., 2024). To fight fraud, we urgently need more resilient and flexible solutions.

In several industries, including financial institutions, e-commerce sites, healthcare providers, and educational institutions, fraudulent activities erode trust, divert resources, and stifle innovation. AI is emerging as revolutionary solutions to address these pervasive issues at this critical juncture (Odeyemi et al., 2024). Conventional fraud detection techniques are becoming less effective. Manual procedures are sluggish, prone to mistakes, and overpowered by fraudsters' constantly changing strategies (Odufisan et al., 2025). Complex patterns concealed in enormous volumes of data are difficult for legacy systems to find (Hilal et al., 2022). AI provides a potent remedy in this situation.

AI is perfect for fraud detection because of its capacity to examine large datasets and spot minute irregularities (Odufisan et al., 2025). To identify trends and forecast future fraudulent activity, machine learning algorithms can be trained on past fraud incidents. This makes it possible to monitor transactions in real time and identify suspect conduct before it has a chance to inflict financial harm (U. Bansal et al., 2024). AI can detect possible fraudulent loans, illegal access attempts, and money laundering schemes in the banking and finance industry by analyzing consumer behavior, spending trends, and account activity (Abdel et al., 2023). This gives financial institutions the ability to prevent losses by taking preventive steps like account freezes or extra authentication procedures.

AI-powered fraud detection has enormous potential benefits for the e-commerce industry (Odufisan et al., 2025). To find questionable orders that might be connected to credit card fraud, AI can examine IP addresses, device fingerprints, and client purchase histories (Gayam & Charles, 2020). AI can also be used to identify fraudulent merchants using e-commerce platforms and detect phony reviews (Paul & Nikolaev, 2021). AI can be used by the healthcare industry to fight identity theft and false claims. AI systems can examine patient data, billing information, and medical records to spot irregularities that might point to fraud (Narne, 2024).

AI can be used by the education sector to fight admission fraud and exam dishonesty. While sophisticated document verification tools can spot faked transcripts and certificates (Boonkrong, 2025), AI-powered proctoring systems can spot suspicious activity during online exams (Nagpal et al., 2024). Additionally, AI can examine student performance data to identify possible instances of plagiarism in essays and tasks (Balalle & Pannilage, 2025; Leong & Zhang, 2025). It is impossible to overestimate the need for AI assistance in the fight against fraud. Countries can protect their economies, foster trust in vital industries, and enable their citizens to confidently engage in a digital future by utilizing AI, and the ability to detect fraud will only advance as it develops, opening the door to more secure and successful nations.

In line with the objectives of this study, several research questions are formulated to guide the conceptual analysis. First, how is the transformation taking place from traditional fraud detection methods to AI-based detection systems? Second, how deep are learning approaches—particularly in the context of artificial intelligence—being applied to enhance fraud detection processes? Third, how adaptive are current AI-based systems in detecting fraud in real-time scenarios? Lastly, how are challenges related to data imbalance and feature engineering being addressed in the development of real-time fraud detection systems?

Methodology

This study employs a theoretical literature review as its primary research method to achieve the stated objectives and explore the role of artificial intelligence (AI) in fraud detection. The literature review approach enables a comprehensive synthesis of existing scholarly works, models, and empirical findings related to AI-driven fraud detection systems across various sectors, particularly finance, e-commerce, healthcare, and education. By systematically identifying, analyzing, and comparing relevant studies, this method provides a foundation for understanding technological trends, algorithmic advancements, and implementation challenges in fraud detection. It also helps in mapping out thematic developments, performance metrics, and key methodological approaches used in the field.

This study draws upon methodological frameworks adopted by previous researchers (Torkayesh et al., 2023; Vasiljeva et al., 2017), which emphasize structured selection criteria, thematic coding, and critical interpretation of secondary sources. The review integrates both conceptual and empirical findings, offering a conceptual framework for future research and practical applications. This approach is particularly suited for emerging topics such as AI in fraud detection, where rapid technological evolution necessitates up-to-date scholarly synthesis rather than primary data collection.

Result And Discussion

Results

In the current research, the authors conceptualize fraud detection as the dependent variable influenced by various dimensions of artificial intelligence (AI) implementation. The relationship is depicted in the conceptual model provided in Figure 1, where AI serves as the primary driver of advancement in fraud detection systems.

The model suggests that fraud detection outcomes are shaped by multiple AI-related components, including machine learning algorithms, deep learning architectures, system adaptability, and the handling of data challenges such as imbalance and feature engineering. These elements collectively form the foundation of AI-based fraud detection mechanisms that differ significantly from traditional rule-based systems.

This theoretical relationship is established based on findings from the reviewed literature, where AI technologies consistently demonstrate superior performance in identifying complex fraud patterns, adapting to new fraud techniques in real-time, and processing vast amounts of transactional data more effectively. For example, studies reviewed in this paper report detection accuracies exceeding 99% using models such as Random Forests, LSTM, and hybrid CNN-LSTM approaches, thereby supporting the proposition that AI significantly enhances fraud detection capabilities.

Thus, the result of this conceptual review confirms that AI not only influences fraud detection performance, but also reshapes the operational logic of detection systems by enabling automation, scalability, and predictive capabilities.

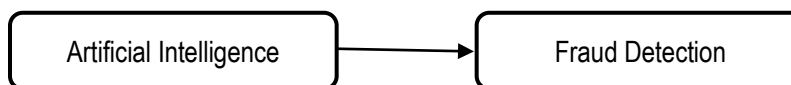


Figure 1. Conceptual model of research

Discussion

The Transformation from Traditional to AI-Based Detection

The complexity and scope of contemporary fraudulent activity have proven to be too much for traditional fraud detection techniques, such as rule-based algorithms and manual inspections (Chukwu & Ebenmelu, 2025). These traditional methods are unable to adequately catch intricate patterns suggestive of fraudulent activity and struggle to keep up with changing fraud tactics. The requirement for real-time detection, increased accuracy, and the capacity to adjust to ever-evolving fraud schemes has fueled the move toward AI-based solutions (Kamisetty, 2024).

AI has transformed the detection of financial fraud by offering more precise, scalable, and adaptable solutions across a few industries, including banking, insurance, e-commerce, and healthcare (Prabin Adhikari et al., 2024). By improving the accuracy and effectiveness of fraud pattern identification, the use of AI approaches in fraud detection produces positive results and significantly advances the area (Yuhertiana & Amin, 2024). AI systems can continuously learn from new data and changing fraud patterns, which makes them much more successful against new threats than traditional methods that rely on static rules and previous trends (Shoetan & Familoni, 2024).

Fraud Detection using Machine Learning Algorithms

The foundation of contemporary fraud detection systems is now machine learning. According to research, machine learning algorithms perform noticeably better than conventional fraud detection techniques in terms of efficiency and accuracy (Kamisetty, 2024). Numerous machine learning models have been successfully implemented, including

unsupervised and semi-supervised methods as well as supervised learning techniques including logistic regression, decision trees, support vector machines (SVM), random forests, and k-nearest neighbors (KNN) (M. Bansal et al., 2022).

These algorithms exhibit remarkable performance. Research has shown that Random Forest algorithms consistently reach high accuracy rates, with credit card fraud detection accuracy levels over 99% (Sun et al., 2024). In a similar vein, research has shown that ensemble approaches that integrate several classifiers perform better, with accuracy rates of 99.96% and precision rates of 99.53% (Khan et al., 2024). These ensemble techniques' efficacy stems from their capacity to take advantage of the complementing qualities of many algorithms, resulting in a more reliable framework for identifying fraudulent transactions (Mohammed & Kora, 2023).

As new patterns appear, machine learning models get better over time and grow more adept at spotting fraud (Sun et al., 2024). These solutions enable quicker reaction times to possible threats, automate previously manual research procedures, and significantly increase fraud detection rates while significantly lowering false positives (Kamisetty, 2024). Financial organizations can save money and improve operational efficiency by reducing false positives by about 30% by integrating cutting-edge machine learning models with traditional techniques (<https://thefintechmag.com/ai-in-fraud-detection-how-banks-reduce-false-positives-by-40>).

Approaches of Deep Learning

The ability to detect fraud has significantly improved because of deep learning. Deep learning models, in contrast to classic machine learning techniques, are capable of processing massive amounts of high-dimensional data and spotting complex patterns that would be challenging for older methods to recognize (Kufel et al., 2023). Deep learning capacity to learn hierarchical representations, identify temporal connections, and efficiently analyze sequential financial data is credited with its success in fraud detection (Chen et al., 2025).

For detecting fraud, Long Short-Term Memory (LSTM) networks have proven to be highly successful, particularly when it comes to capturing the temporal patterns present in financial transactions (Al-Selwi et al., 2024). The better capacity of LSTM models to detect fraud while reducing false positives is demonstrated by their accuracy rates of 99.38%, precision of 99.40%, recall of 99.22%, and F1-scores of 99.31% (Al-Selwi et al., 2024). Additionally, Convolutional Neural Networks (CNNs) have demonstrated great promise, especially when it comes to identifying abnormalities and geographical patterns in transaction data [(Ersavas et al., 2024).

Even more successful are hybrid deep learning techniques that combine many architectures. For example, when it comes to detecting fraudulent transactions, CNN and LSTM network combinations outperform individual models (Bamber et al., 2025). By learning to recreate valid transactions and recognizing deviations based on reconstruction errors, autoencoders, unsupervised deep learning models, have proven very useful in finding abnormalities (Neloy & Turgeon, 2024). Accuracy of 99.48%, precision of 99.39%, recall of 99.55%, and false positive rates as low as 0.599% are attained when Variational Autoencoders (VAE) and Transformer networks are combined (Zhou et al., 2024).

Adaptive Systems and Real-Time Fraud Detection

The ability of AI-driven fraud detection to process data in real time is one of its most important benefits. With continuous training on patterns and abnormalities in consumer transactions, generative AI has become a cutting-edge system that can identify suspicious activity in real-time (Zhang et al., 2025). Financial institutions need real-time fraud detection techniques because they allow for the prompt discovery and stopping of fraudulent activity (Immadisetty, 2024).

The cutting edge of fraud detection technology is represented by adaptive machine learning models. By learning from

fresh data and adapting to new fraud patterns, these systems are built to continuously change (Ikemefuna et al., 2024). They use sophisticated algorithms like reinforcement learning, which continuously improves decision-making processes and enhance detection tactics by getting feedback on activities. These systems can update gradually as each transaction becomes available thanks to online learning capabilities, guaranteeing that they stay up to date and adaptable to new threats (Ikemefuna et al., 2024).

Feature Engineering and Handling Data Imbalance

Data imbalance is a recurring problem in fraud detection since fraudulent transactions usually make up a small portion of all transactions. Researchers use methods such as Adaptive Synthetic Sampling (ADASYN) and Synthetic Minority Over-sampling Technique (SMOTE) to address this (Bello et al., 2025). Studies have demonstrated that appropriate data balance can boost recall by 10.37% when compared to baseline techniques, demonstrating the great efficacy of SMOTE-based approaches (Matharaarachchi et al., 2024). To improve model performance, feature engineering and data preparation are essential (<https://machinelearningmastery.com/the-concise-guide-to-feature-engineering-for-better-model-performance>). Research has shown that selecting features carefully and using the right data preprocessing methods greatly improves the accuracy of fraud detection. With sensitivity and specificity scores of 0.997 and 0.994, respectively, hybrid feature-selection algorithms that combine filter and wrapper approaches guarantee that only pertinent features are used for machine learning (Hsu et al., 2011).

Challenges in AI-Driven Fraud Detection

AI-driven fraud detection has come a long way, but there are still several important obstacles to overcome. Because AI models might inherit biases from training data and provide discriminatory results, algorithmic bias is a serious concern (Yuhertiana & Amin, 2024). Concerns about data security and privacy are crucial, especially as financial data is sensitive (Kamisetty, 2024). AI systems' complexity and lack of transparency provide difficulties, particularly when judgments made by AI have a big influence on consumers (Olorunniwo et al., 2025).

Interpretability of models continues to be a significant concern. Despite deep learning models' excellent accuracy, stakeholders find it challenging to comprehend how fraud decisions are made due to their "black box" nature [(Qamar & Bawany, 2023). To address this issue, explainable AI (XAI) methods like LIME and SHAP have been developed, offering more lucid explanations of model choices, and finding influential elements in the model is made easier by the incorporation of XAI (Salih et al., 2025).

Financial firms must constantly adjust to changing regulatory frameworks for AI in banking, which adds another level of complexity to regulatory compliance (Olorunniwo et al., 2025). For many firms, the expense of deploying cutting-edge technology and the difficulties of integrating them with current systems continue to be practical considerations (Haber & Carmeli, 2023).

Applications Across Financial Sectors

AI-powered fraud detection has been effectively applied in a variety of financial fields. These tools have greatly improved real-time transaction monitoring and consumer behavior analysis in the banking industry, assisting organizations in spotting irregularities suggestive of fraud (Olorunniwo et al., 2025). Machine learning techniques have made it possible to detect fraudulent claims more accurately in the insurance industry. Studies have shown that detection rates have improved by a factor of 4.2 (84% recall for a positive rate of 20%) (du Preez et al., 2025).

By combining natural language processing and deep learning approaches, AI algorithms in fintech and payment systems have demonstrated remarkable efficacy in detecting intricate and subtle fraudulent behaviors (Shoetan & Familoni, 2024). AI has also greatly aided in the identification of healthcare insurance fraud; random forest classifiers

have achieved 98.21% accuracy, 98.08% precision, and 100% flawless recall (du Preez et al., 2025).

Emerging Technologies and Future Directions

The field is seeing the emergence of several interesting directions. Blockchain technology in conjunction with federated learning provides solutions for highly accurate fraud detection while protecting privacy (Yurdem et al., 2024). By collecting relationships between entities and using network analysis to find suspicious patterns, graph-based machine learning techniques hold great promise for financial network fraud detection (Kotiyal et al., 2024). To improve openness and stakeholder trust, Explainable Artificial Intelligence (XAI) is being incorporated into fraud detection systems more frequently (Faruk et al., 2025). Research on how various quantum feature maps and ansatz configurations impact the effectiveness of quantum-based classifiers for fraud detection is part of the developing field of quantum machine learning (Devadas & T, 2025).

Conclusions and Recommendation

The integration of artificial intelligence (AI) into fraud detection represents a significant advancement in enhancing financial security across various sectors. This study concludes that AI-driven fraud detection systems offer superior accuracy, adaptability, and efficiency compared to traditional rule-based approaches. Machine learning and deep learning models enable organizations to identify complex fraud patterns and respond dynamically to evolving fraudulent behaviors.

Despite these advantages, the successful implementation of AI-based fraud detection systems depends on addressing critical challenges, including data quality, model interpretability, algorithmic transparency, regulatory compliance, and ethical considerations. The findings suggest that organizations should adopt explainable AI techniques, strengthen data governance frameworks, and employ hybrid detection models that combine traditional rules with advanced AI algorithms. Furthermore, continuous learning mechanisms and close collaboration among AI developers, domain experts, and regulators are essential to ensure responsible, effective, and legally compliant fraud detection systems.

Limitation

Despite its contributions, this study has several limitations that should be acknowledged. First, the research is based on a theoretical literature review and does not incorporate empirical testing or primary data collection. Consequently, the conclusions rely on the synthesis of existing studies, which may limit the generalizability of the findings. Second, the proposed conceptual framework has not been empirically validated using quantitative methods or real-world case studies. Its applicability may therefore differ across industries, organizational scales, and geographic or regulatory contexts. Finally, the rapidly evolving nature of artificial intelligence technologies presents a challenge in maintaining the relevance of the reviewed literature. Advances in algorithms, computational techniques, and regulatory standards may quickly outpace existing studies. Future research is encouraged to conduct empirical validation through case studies, experiments, or simulations and to explore sector-specific implementations of AI-based fraud detection systems.

Research Contribution

This study makes several important contributions to both academic literature and practical applications. Academically, it enriches the fraud detection and information systems literature by developing a comprehensive conceptual framework that explains the role of artificial intelligence in enhancing fraud detection capabilities. By synthesizing prior research across multiple sectors—including finance, e-commerce, healthcare, and education—this study provides a holistic understanding of how AI improves accuracy, scalability, and adaptability in fraud prevention.

From a practical perspective, the study offers actionable insights for practitioners by identifying key AI components,

such as machine learning algorithms, deep learning models, hybrid detection systems, and real-time learning mechanisms. These insights can support organizations in designing and implementing more effective AI-driven fraud detection strategies. Additionally, the formulation of clear research directions provides a foundation for future empirical studies aimed at validating and extending the proposed framework.

References

- Abdel, L., Aziz, R., & Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *RCBA*, 6(1), 110–132. <https://orcid.org/0000-0003-3394-5222>
- Abhulimen, O., & Erastus, O. (2022). Automatic Age Estimation of Persons with Dark Skin Tone Using Deep Learning Approach. *International Journal of Computing and Digital Systems*, 12, 1184–1189. <https://doi.org/10.12785/ijcds/120194>
- Ahmad, S. F., Alam, M. M., Rahmat, M. K., Mubarik, M. S., & Hyder, S. I. (2022). Academic and Administrative Role of Artificial Intelligence in Education. In *Sustainability (Switzerland)* (Vol. 14, Issue 3). MDPI. <https://doi.org/10.3390/su14031101>
- Ahmad, S. F., Rahmat, M. K., Mubarik, M. S., Alam, M. M., & Hyder, S. I. (2021). Artificial intelligence and its role in education. *Sustainability (Switzerland)*, 13(22). <https://doi.org/10.3390/su132212902>
- Al-Selwi, S. M., Hassan, M. F., Abdulkadir, S. J., Muneer, A., Sumiea, E. H., Alqushaibi, A., & Ragab, M. G. (2024). RNN-LSTM: From applications to modeling techniques and beyond—Systematic review. *Journal of King Saud University - Computer and Information Sciences*, 36(5), 102068. <https://doi.org/10.1016/J.JKSUCI.2024.102068>
- Amos Kipnetich. (2025). A review of online scams and financial frauds in the digital age. *GSC Advanced Research and Reviews*, 22(1), 302–329. <https://doi.org/10.30574/gscarr.2025.22.1.0025>
- Balalle, H., & Pannilage, S. (2025). Reassessing academic integrity in the age of AI: A systematic literature review on AI and academic integrity. *Social Sciences & Humanities Open*, 11, 101299. <https://doi.org/10.1016/J.SSAHO.2025.101299>
- Bamber, S. S., Katkuri, A. V. R., Sharma, S., & Angurala, M. (2025). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. *Computers & Security*, 148, 104146. <https://doi.org/10.1016/J.COSE.2024.104146>
- Bansal, M., Goyal, A., & Choudhary, A. (2022). A comparative analysis of K-Nearest Neighbor, Genetic, Support Vector Machine, Decision Tree, and Long Short Term Memory algorithms in machine learning. *Decision Analytics Journal*, 3, 100071. <https://doi.org/10.1016/J.DAJOUR.2022.100071>
- Bansal, U., Bharatwal, S., Bagiyam, D. S., & Kismawadi, E. R. (2024). Fraud detection in the era of AI: Harnessing technology for a safer digital economy. In *AI-Driven Decentralized Finance and the Future of Finance* (pp. 143–164). IGI Global. <https://doi.org/10.4018/979-8-3693-6321-8.ch006>
- Bello, D., Okunola, A., & Fatima, A. (2025). *Addressing the Challenges of Imbalanced Datasets in AI-Driven Fraud Detection*.
- Boonkrong, S. (2025). Design of an academic document forgery detection system. *International Journal of Information Technology*, 17(9), 5175–5187. <https://doi.org/10.1007/s41870-024-02006-6>
- Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications. *Data Science and Management*. <https://doi.org/10.1016/J.DSM.2025.08.002>
- Chukwu, B. N., & Ebenmelu, C. E. (2025). Artificial Intelligence and Fraud Detection in US Commercial Banks: Opportunities and Challenges. *World Journal of Advanced Research and Reviews*, 27(3), 1083–1091. <https://doi.org/10.30574/wjarr.2025.27.3.3259>
- Devadas, R. M., & T, S. (2025). Quantum machine learning: A comprehensive review of integrating AI with quantum computing for computational advancements. In *MethodsX* (Vol. 14). Elsevier B.V. <https://doi.org/10.1016/j.mex.2025.103318>
- du Preez, A., Bhattacharya, S., Beling, P., & Bowen, E. (2025). Fraud detection in healthcare claims using machine

- learning: A systematic review. *Artificial Intelligence in Medicine*, 160, 103061. <https://doi.org/10.1016/J.ARTMED.2024.103061>
- Ersavas, T., Smith, M. A., & Mattick, J. S. (2024). Novel applications of Convolutional Neural Networks in the age of Transformers. *Scientific Reports*, 14(1), 10000. <https://doi.org/10.1038/s41598-024-60709-z>
- Faruk, N., Tariq, A., Oladele, S., & Gok, M. (2025). *Explainable AI (XAI) for Fraud Detection: Building Trust and Transparency in AI-Driven Financial Security Systems*.
- Gayam, S., & Charles, E. (2020). AI-Driven Fraud Detection in E-Commerce: Advanced Techniques for Anomaly Detection, Transaction Monitoring, and Risk Mitigation. *Distrib. Learn. Broad Appl. Sci. Res.*, 124–151.
- Haber, L., & Carmeli, A. (2023). Leading the challenges of implementing new technologies in organizations. *Technology in Society*, 74, 102300. <https://doi.org/10.1016/J.TECHSOC.2023.102300>
- Helmy Mohamad, A., Farouk Hassan, G., & S. Abd Elrahman, A. (2022). Impacts of e-commerce on planning and designing commercial activities centers: A developed approach. *Ain Shams Engineering Journal*, 13(4), 101634. <https://doi.org/10.1016/j.asej.2021.11.003>
- Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, 11(1), 1130. <https://doi.org/10.1057/s41599-024-03606-0>
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications*, 193, 116429. <https://doi.org/10.1016/J.ESWA.2021.116429>
- Hsu, H. H., Hsieh, C. W., & Lu, M. Da. (2011). Hybrid feature selection by combining filters and wrappers. *Expert Systems with Applications*, 38(7), 8144–8150. <https://doi.org/10.1016/J.ESWA.2010.12.156>
- Ikemefuna, D., Okusi, O., Chibuzor, A., & Yusuf, S. (2024). *Adaptive Fraud Detection Systems: Using Machine Learning To Identify and Respond To Evolving Financial Threat*. <https://doi.org/10.56726/IRJMETS61738>
- Immadisetty, A. (2024). *Real-Time Fraud Detection Using Streaming Data in Financial Transactions*. 66–76. <https://doi.org/10.70589/JRTCSE.2025.13.1.9>
- Kamisetty, R. (2024). Artificial Intelligence in Banking Fraud Detection: Enhancing Security Through Intelligent Systems Rajesh Kamisetty. *International Journal for Multidisciplinary Research (IJFMR)*, 6(6), 1–14. www.ijfmr.com
- Khan, A. A., Chaudhari, O., & Chandra, R. (2024). A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation. *Expert Systems with Applications*, 244, 122778. <https://doi.org/10.1016/J.ESWA.2023.122778>
- Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, 126, 221–238. <https://doi.org/10.1016/j.jbusres.2020.12.006>
- Kotiyal, A., Hussein, L., Deepak, A., Rana, A., Manjunatha, Dixit, K. K., & Reddy, R. A. (2024). Graph-Based Machine Learning Approaches for Fraud Detection in Financial Networks. *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, 7, 1714–1720. <https://doi.org/10.1109/IC3I61595.2024.10828743>
- Kufel, J., Bargiel-Łączek, K., Kocot, S., Koźlik, M., Bartnikowska, W., Janik, M., Czogalik, Ł., Dudek, P., Magiera, M., Lis, A., Paszkiewicz, I., Nawrat, Z., Cebula, M., & Gruszczńska, K. (2023). What Is Machine Learning, Artificial Neural Networks and Deep Learning?—Examples of Practical Applications in Medicine. In *Diagnostics* (Vol. 13, Issue 15). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/diagnostics13152582>
- Leong, W. Y., & Zhang, J. (2025). AI on Academic Integrity and Plagiarism Detection. *ASM Science Journal*, 20, 2025. <https://doi.org/10.32802/asmscj.2025.1918>
- Liu, Q., Hagenmeyer, V., & Keller, H. (2021). A Review of Rule Learning Based Intrusion Detection Systems and Their Prospects in Smart Grids. *IEEE Access*, PP, 1. <https://doi.org/10.1109/ACCESS.2021.3071263>
- Matharaarachchi, S., Domaratzki, M., & Muthukumarana, S. (2024). Enhancing SMOTE for imbalanced data with

- abnormal minority instances. *Machine Learning with Applications*, 18, 100597. <https://doi.org/10.1016/J.MLWA.2024.100597>
- Mohammed, A., & Kora, R. (2023). A comprehensive review on ensemble deep learning: Opportunities and challenges. *Journal of King Saud University - Computer and Information Sciences*, 35(2), 757–774. <https://doi.org/10.1016/J.JKSUCI.2023.01.014>
- Nagpal, N., Srivastava, A., & Verma, P. (2024). AI-Powered Proctoring: Safeguarding Online Assessment in the Education 5.0. In T. Singh, S. Dutta, S. Vyas, & Á. Rocha (Eds.), *Explainable AI for Education: Recent Trends and Challenges* (pp. 271–285). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72410-7_15
- Narne, H. (2024). Machine Learning for Health Insurance Fraud Detection: Techniques, Insights, and Implementation Strategies. *International Journal of Research and Analytical Reviews*, 709. www.ijrar.org
- Neloy, A. A., & Turgeon, M. (2024). A comprehensive study of auto-encoders for anomaly detection: Efficiency and trade-offs. *Machine Learning with Applications*, 17, 100572. <https://doi.org/10.1016/J.MLWA.2024.100572>
- Odeyemi, O., Mhlongo, N., Nwankwo, E., & Soyombo, O. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, 11, 2101–2110. <https://doi.org/10.30574/ijrsra.2024.11.1.0279>
- Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology*, 7, 100127. <https://doi.org/10.1016/j.jeconc.2025.100127>
- Olorunniwo, O., Alomge, M., & Isreal, O. (2025). *Transparency vs. Complexity in AI Systems*.
- Olufemi, B., Bello, O., Olufemi, K., & Author, C. (2024). *Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities*. 5, 1505–1520. <https://doi.org/10.51594/csitrj.v5i6.1252>
- Paul, H., & Nikolaev, A. (2021). Fake review detection on online E-commerce platforms: a systematic literature review. *Data Mining and Knowledge Discovery*, 35(5), 1830–1881. <https://doi.org/10.1007/s10618-021-00772-6>
- Prabin Adhikari, Prashamsa Hamal, & Francis Baidoo Jnr. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*, 13(1), 1457–1472. <https://doi.org/10.30574/ijrsra.2024.13.1.1860>
- Qamar, T., & Bawany, N. Z. (2023). Understanding the black-box: towards interpretable and reliable deep learning models. *PeerJ Computer Science*, 9. <https://doi.org/10.7717/peerj-cs.1629>
- Ran, D., Yingli, W., & Haoxin, Q. (2020). Artificial intelligence speech recognition model for correcting spoken English teaching. *Journal of Intelligent & Fuzzy Systems*, 40, 1–12. <https://doi.org/10.3233/JIFS-189388>
- Salih, A. M., Raisi-Estabragh, Z., Galazzo, I. B., Radeva, P., Petersen, S. E., Lekadir, K., & Menegaz, G. (2025). A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. *Advanced Intelligent Systems*, 7(1), 2400304. <https://doi.org/https://doi.org/10.1002/aisy.202400304>
- Shoetan, P. O., & FAMILONI, B. T. (2024). TRANSFORMING FINTECH FRAUD DETECTION WITH ADVANCED ARTIFICIAL INTELLIGENCE ALGORITHMS. *Finance & Accounting Research Journal*. <https://api.semanticscholar.org/CorpusID:269233906>
- Su, H., Jiang, I. M., & Liu, D. (2025). Detecting financial fraud risk using machine learning: Evidence based on different categories and matching samples. *Finance Research Letters*, 85, 107858. <https://doi.org/10.1016/J.FRL.2025.107858>
- Sun, Z., Wang, G., Li, P., Wang, H., Zhang, M., & Liang, X. (2024). An improved random forest based on the classification accuracy and correlation measurement of decision trees. *Expert Systems with Applications*, 237, 121549. <https://doi.org/10.1016/J.ESWA.2023.121549>
- Theodorakopoulos, L., Theodoropoulou, A., & Stamatiou, Y. (2024). A State-of-the-Art Review in Big Data Management Engineering: Real-Life Case Studies, Challenges, and Future Research Directions. In *Eng* (Vol. 5, Issue 3, pp. 1266–1297). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/eng5030068>

- Torkayesh, A. E., Tirkolaee, E. B., Bahrini, A., Pamuar, D., & Khakbaz, A. (2023). A Systematic Literature Review of MABAC Method and Applications: An Outlook for Sustainability and Circularity. *Informatica*, 34, 415–448. <https://api.semanticscholar.org/CorpusID:257274475>
- Vasiljeva, T., Shaikhulina, S., & Kreslins, K. (2017). Cloud Computing: Business Perspectives, Benefits and Challenges for Small and Medium Enterprises (Case of Latvia). *Procedia Engineering*, 178, 443–451. <https://doi.org/https://doi.org/10.1016/j.proeng.2017.01.087>
- Yuhertiana, I., & Amin, A. H. (2024). Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review. *KnE Social Sciences*. <https://api.semanticscholar.org/CorpusID:271012292>
- Yurdem, B., Kuzlu, M., Gullu, M. K., Catak, F. O., & Tabassum, M. (2024). Federated learning: Overview, strategies, applications, tools and future directions. *Heliyon*, 10(19), e38137. <https://doi.org/10.1016/J.HELİYON.2024.E38137>
- Zhang, Z., Zhang, J., Zhang, X., & Mai, W. (2025). A comprehensive overview of Generative AI (GAI): Technologies, applications, and challenges. *Neurocomputing*, 632, 129645. <https://doi.org/10.1016/j.neucom.2025.129645>
- Zhou, C., Li, Z., Song, J., & Xiang, W. (2024). TransVAE-DTA: Transformer and variational autoencoder network for drug-target binding affinity prediction. *Computer Methods and Programs in Biomedicine*, 244, 108003. <https://doi.org/10.1016/J.CMPB.2023.108003>