

Is Artificial Intelligence a positive variable in detecting financial fraud?Author: Luca Bassil¹*Affiliation:*

1. *Business School, Holy Spirit University of Kaslik, P.O. Box 446, Jounieh, Lebanon*
2. *CIRAME Research Center, Holy Spirit University of Kaslik, P.O. Box 446, Jounieh, Lebanon*

Abstract:

Financial fraud has become an important challenge for banks, financial institutions, businesses, and consumers. As financial transactions increasingly move online, fraudsters have developed more sophisticated methods of stealing money and manipulating financial systems. Traditional fraud detection systems often rely on predefined rules, while artificial intelligence can analyze large amounts of transaction data and identify unusual patterns. This research examines whether artificial intelligence is genuinely helpful in detecting financial fraud. The study uses secondary evidence from recent academic research and systematic literature reviews concerning artificial intelligence, machine learning, and financial fraud detection. The findings indicate that AI can improve fraud detection by identifying complex patterns, processing large volumes of transactions, and adapting to certain types of fraudulent behavior. Machine-learning techniques such as random forests, gradient-boosting models, neural networks, and anomaly-detection methods have demonstrated strong performance in different fraud-detection applications. However, AI is not a perfect solution. Fraud datasets are often highly imbalanced, fraudulent behavior changes over time, and some advanced AI models are difficult to explain. False positives can also create problems by incorrectly flagging legitimate transactions. Therefore, the evidence suggests that AI is a useful tool for fraud detection, but its effectiveness depends on data quality, model design, continuous monitoring, and human oversight. AI is most appropriately viewed as an enhancement to fraud-detection systems rather than a complete replacement for human investigators and traditional controls.

Keywords:

Artificial Intelligence, Fraud Detection, Machine Learning, Financial Fraud, Banking, Cybersecurity, Anomaly Detection, Financial Crime

Introduction:

Financial fraud is a major problem for financial institutions and businesses around the world. Fraud can take many forms, including credit-card fraud, identity theft, account takeover, insurance fraud, financial statement manipulation, payment fraud, and money laundering. The rapid growth of digital banking and online transactions has created new opportunities for legitimate financial activity, but it has also created additional opportunities for fraudulent behavior.

Traditional fraud-detection systems generally rely on predefined rules. For example, a bank may flag a transaction when it exceeds a certain amount, occurs in an unusual location, or differs significantly from a customer's normal behavior. These systems can be effective for known types of fraud, but they can struggle when fraudsters change their techniques.

Artificial intelligence provides another approach. Instead of relying entirely on predefined rules, machine-learning systems can analyze historical transaction data and identify patterns associated with fraudulent behavior. AI can process very large quantities of transactions and can potentially identify relationships that would be difficult for humans to recognize manually.

Recent research has shown that machine-learning and deep-learning techniques are increasingly being applied to financial fraud detection. A 2024 systematic literature review found that models such as XGBoost, LightGBM, and Random Forest frequently demonstrate strong performance in banking fraud detection. The review also identified credit-card fraud, identity theft, and account takeover as important applications.

However, the effectiveness of AI should not be assumed simply because an AI model produces a high level of accuracy. Fraud detection presents several unique challenges. Fraudulent transactions generally represent a very small proportion of total transactions, creating an imbalance between fraudulent and legitimate observations. In addition, fraudsters continuously change their methods, meaning that a model trained on historical behavior may become less effective over time. Recent reviews also identify explainability, privacy, data imbalance, and compliance as important challenges for AI-based fraud detection.

Therefore, this research examines whether AI is genuinely helpful in detecting financial fraud and whether it can improve upon traditional fraud-detection approaches.

1.1 Research Questions

This research addresses the following questions:

1. Can artificial intelligence improve the detection of financial fraud?
2. How does AI-based fraud detection compare with traditional rule-based systems?
3. Which machine-learning techniques are commonly used to detect fraud?
4. What are the main limitations of using AI for fraud detection?
5. Can AI completely replace human involvement in fraud detection?

1.2 Research Objectives

The objectives of this research are to:

- Examine the role of artificial intelligence in financial fraud detection.
- Analyze empirical evidence concerning the effectiveness of AI-based fraud-detection systems.
- Compare AI-based approaches with traditional fraud-detection methods.
- Identify the main advantages of machine learning and deep learning in fraud detection.
- Examine the limitations and risks associated with AI-based fraud detection.

- Determine whether AI should replace traditional fraud-detection methods or be used alongside them.

1.3 Research Gap

A large amount of research has examined whether artificial intelligence can detect fraudulent transactions. However, many studies focus on the technical performance of individual models rather than the broader question of whether AI provides a reliable solution in real-world financial systems.

A model may perform very well on a particular dataset but face difficulties when used with new customers, new types of fraud, or changing transaction patterns. Furthermore, high predictive accuracy does not necessarily mean that the system is practical for a bank if it produces too many false alerts or cannot explain why a transaction was flagged.

Recent research continues to identify data imbalance, concept drift, limited labeled data, and the trade-off between detection performance and interpretability as important challenges.

This research addresses this gap by examining both the benefits and limitations of AI rather than focusing only on the accuracy of individual models.

Literature Review:

2.1 Financial Fraud

Financial fraud involves intentional deception designed to obtain financial benefits or cause financial losses. Fraud can occur through many channels and can affect individuals, companies, banks, insurance companies, and governments.

Some common types of financial fraud include:

- Credit-card fraud
- Identity theft
- Account takeover
- Online payment fraud
- Loan fraud
- Insurance fraud
- Financial statement fraud
- Money laundering
- Investment fraud

The increasing use of digital financial services has created large quantities of transaction data. This creates both a challenge and an opportunity. The challenge is that financial institutions must monitor enormous numbers of transactions, while the opportunity is that this data can be analyzed using AI and machine-learning systems.

2.2 Traditional Fraud Detection

Traditional fraud-detection systems often use predefined rules to identify suspicious transactions.

For example, a financial institution may create a rule that flags a transaction when:

- The transaction amount is unusually large.
- A customer suddenly makes transactions in a different country.
- Multiple transactions occur within a very short period.

- A customer's behavior changes significantly.
- A transaction occurs in a location associated with previous fraud.

Rule-based systems have an important advantage because their decisions are relatively easy to understand. Investigators can usually identify which rule caused a transaction to be flagged.

However, traditional systems can have difficulty identifying new types of fraud that do not match existing rules. Fraudsters can also modify their behavior to avoid known detection criteria.

2.3 Artificial Intelligence and Machine Learning

Machine learning allows computer systems to identify patterns from data and use these patterns to make predictions or classifications.

Artificial intelligence and blockchain technology may enhance the performance of companies, especially SME's (Khalife et al., 2024), however for this to work, especially in vulnerable environments, government support through proper governance is needed (Athari et al., 2023), combined with proper business experience and entrepreneurial knowledge (Chaanine et al., 2023), this research therefore detects a triad, between technology, governments and individuals that together may positively attribute in an increase in financial reporting quality and better financial transparency (Saber & Sassine, 2022). AI may have revolutionized the Audit industry (Sawaya et al., 2026), but companies with a lack of internal audit and internal controls may not benefit from this technological surge. Furthermore, AI integration does not directly reflect in company growth (Athari et al., 2026) even in data driven cultures (Azoury et al., 2024). Finally, on a post fraudulent action basis, it is worth noting that the increase in technology may help achieve a more accurate pricing (Khalife et al., 2023), rendering earning manipulation less lucrative.

In fraud detection, a machine-learning model can analyze information such as:

- Transaction amount
- Transaction frequency
- Time of transaction
- Geographic location
- Merchant information
- Customer behavior
- Device information
- Previous transaction history

The model can then estimate whether a transaction resembles previously identified fraudulent activity.

This approach can be more flexible than a system based entirely on fixed rules because the model can learn relationships from historical data.

2.4 Supervised Learning

Supervised learning uses historical observations for which the outcome is already known.

For example, a bank may have historical transactions classified as either legitimate or fraudulent. A machine-learning model can learn patterns from these examples and then use those patterns to classify new transactions.

Common supervised-learning models used in fraud detection include:

- Logistic regression
- Decision trees
- Random Forest
- Support Vector Machines
- XGBoost
- LightGBM
- Neural networks

A 2024 systematic literature review of banking fraud detection found that models such as XGBoost, LightGBM, and Random Forest frequently demonstrated strong performance across different fraud-detection applications.

2.5 Unsupervised Learning and Anomaly Detection

Not all fraudulent transactions are known in advance. This creates a problem for supervised learning because a model cannot easily learn from fraud examples that have never been identified.

Unsupervised learning provides another approach. Instead of relying entirely on previously labeled fraudulent transactions, the system attempts to identify unusual patterns or observations.

For example, if a customer normally makes small local purchases but suddenly performs several large transactions from unusual locations, the system may identify this behavior as an anomaly.

Anomaly detection can therefore be particularly useful for identifying previously unknown types of fraud.

2.6 Deep Learning

Deep learning is a branch of machine learning that uses neural networks with multiple layers. These models can process complex relationships and large datasets.

Deep-learning techniques used in financial fraud detection include:

- Convolutional neural networks
- Recurrent neural networks
- Long short-term memory networks
- Autoencoders
- Transformer-based models

A 2025 systematic review examined 108 peer-reviewed studies on deep learning in financial fraud detection. It found that deep-learning methods are being applied across areas including credit cards, insurance, and financial reporting. The review also identified data imbalance, explainability, automation, and privacy compliance as important challenges.

2.7 AI and Credit-Card Fraud Detection

Credit-card fraud is one of the most commonly studied applications of AI-based fraud detection.

Credit-card companies process enormous numbers of transactions. Because most transactions are legitimate, identifying a relatively small number of fraudulent transactions creates a highly imbalanced dataset.

A systematic review published in 2025 examined AI-enhanced techniques for credit-card fraud detection and found that machine learning, deep learning, and optimization techniques are increasingly being used to improve detection systems.

AI can analyze transaction characteristics and identify patterns associated with fraud much faster than a human could manually review every transaction.

2.8 AI and Money Laundering Detection

Artificial intelligence is also being used to detect money laundering.

Money laundering can involve complex networks of transactions designed to hide the origin of illegally obtained funds. This makes it difficult to detect using simple transaction rules.

AI systems can analyze relationships between accounts, transactions, customers, and organizations. Machine learning and network-based methods can therefore help identify unusual transaction patterns.

A 2025 review of AI applications for money-laundering detection examined supervised learning, unsupervised learning, deep learning, and social-network analysis as approaches for identifying suspicious activity.

2.9 Advantages of AI in Fraud Detection

2.9.1 Processing Large Amounts of Data

One of the main advantages of AI is its ability to analyze very large datasets.

Financial institutions may process millions of transactions. Human investigators cannot manually examine every transaction, while automated AI systems can analyze transactions continuously.

2.9.2 Identifying Complex Patterns

Fraud can involve relationships between several variables. AI can identify patterns that may not be obvious when each variable is considered separately.

2.9.3 Real-Time Detection

AI systems can analyze transactions as they occur. This can allow financial institutions to identify suspicious transactions before additional fraudulent activity occurs.

2.9.4 Adaptability

Machine-learning systems can be updated using new data. This can help them respond to changes in fraudulent behavior.

2.9.5 Reducing Manual Work

AI can automatically review transactions and prioritize suspicious cases for human investigators. This allows investigators to concentrate their time on cases that require further examination.

Methodology:

3.1 Research Design

This research uses a quantitative and comparative research design based on secondary empirical evidence.

The research does not create a new fraud-detection model. Instead, it examines findings from existing academic research and systematic literature reviews.

The study compares AI-based fraud detection with traditional approaches and evaluates both the benefits and limitations of AI.

3.2 Data Sources

The research uses secondary data from peer-reviewed academic studies and systematic literature reviews.

The main sources include:

- Yanto, Lisah, and Tandra (2024), which reviews machine-learning models used for banking fraud detection.
- Hernandez Aros et al. (2024), which reviews machine-learning applications for financial fraud detection.
- Hafez et al. (2025), which reviews AI-enhanced techniques for credit-card fraud detection.
- A 2025 systematic review of deep learning in financial fraud detection.
- Zafar and Wu (2026), which examines methodological challenges associated with explainable AI in fraud detection.
- Recent research concerning AI applications in money-laundering detection.

These studies were selected because they examine fraud detection across different financial applications and provide evidence concerning both performance and limitations.

3.3 Variables

The research considers several important variables.

Detection Accuracy

Detection accuracy represents the ability of a system to correctly classify fraudulent and legitimate transactions.

Precision

Precision represents the proportion of transactions identified as fraudulent that are actually fraudulent. High precision is important because a system that generates many incorrect alerts can create unnecessary work for investigators and inconvenience legitimate customers.

Recall

Recall measures how effectively the system identifies actual fraudulent transactions. A system with low recall may fail to detect significant amounts of fraud.

False Positives

A false positive occurs when a legitimate transaction is incorrectly identified as fraudulent.

False positives are particularly important in banking because excessive alerts can inconvenience customers and increase the workload of fraud investigators.

False Negatives

A false negative occurs when a fraudulent transaction is incorrectly classified as legitimate.

False negatives are potentially costly because they represent fraudulent activity that the detection system failed to identify.

Processing Speed

Processing speed refers to how quickly a fraud-detection system can analyze transactions and produce alerts.

This is particularly important for real-time payment systems.

3.4 Evaluation Approach

The research compares findings across different AI-based fraud-detection studies.

The analysis considers:

- The type of AI model used.
- The type of fraud examined.
- The dataset used.
- The reported detection performance.
- The ability to identify new fraud patterns.
- The occurrence of false positives.
- The interpretability of the model.
- The practical challenges associated with implementation.

Because the studies use different datasets and methodologies, the research does not combine their results into a single statistical measurement.

Instead, the study identifies common findings across the existing literature.

3.5 Methodological Limitations

Several limitations should be considered.

First, different studies use different datasets. A model that performs well on one dataset may not achieve the same performance in another environment.

Second, fraud datasets are often highly imbalanced because legitimate transactions greatly outnumber fraudulent ones. This means that accuracy alone may provide an incomplete picture of model performance.

Third, fraudulent behavior changes over time. A model trained using historical fraud patterns may become less effective when fraudsters develop new techniques.

Finally, some advanced AI models are difficult to explain. This creates challenges for financial institutions that need to justify why a transaction was flagged.

Recent research specifically identifies the "black box" nature of complex AI systems as an important issue for transparency, trust, and regulatory compliance.

Results:

4.1 Overall Effectiveness of AI

The reviewed evidence indicates that AI can improve fraud-detection capabilities.

Machine-learning systems can identify patterns across large numbers of transactions and can detect relationships that may be difficult to capture using predefined rules.

A systematic review of banking fraud-detection models found strong performance from several machine-learning approaches, including XGBoost, LightGBM, and Random Forest. Hybrid approaches combining multiple techniques also showed strong results in the studies reviewed. However, the results vary across datasets and applications. Therefore, no single AI model can be identified as universally effective for every type of financial fraud.

4.2 Comparison Between Traditional and AI-Based Detection

Table 1. Traditional Fraud Detection vs. AI-Based Fraud Detection

Feature	Traditional Rule-Based Systems	AI-Based Systems
Decision process	Predefined rules	Patterns learned from data
Large-scale processing	Limited compared with AI	Highly suitable
Detection of known fraud	Effective	Effective
Detection of new patterns	Often limited	Potentially stronger
Adaptability	Requires manual rule changes	Can learn from new data
Explainability	Usually high	Can be limited
False positives	Can be significant	Can potentially be reduced
Human involvement	High	Still required
Real-time monitoring	Possible	Highly suitable

The comparison shows that AI can provide advantages in flexibility and large-scale data processing. However, traditional systems remain useful because their decisions are generally easier to understand and audit.

4.3 Machine-Learning Models

Research indicates that different machine-learning models have different strengths.

Table 2. Common AI Techniques Used in Fraud Detection

Model	Typical Application	Main Characteristic
Logistic Regression	Transaction classification	Relatively simple and interpretable

Decision Trees	Fraud classification	Easy to understand
Random Forest	Banking and payment fraud	Strong classification performance
XGBoost	Banking fraud	Strong predictive performance
LightGBM	Large transaction datasets	Efficient processing
Neural Networks	Complex fraud patterns	Can model complex relationships
Autoencoders	Anomaly detection	Useful for unusual behavior
LSTM Networks	Transaction sequences	Can analyze patterns over time

The literature does not demonstrate that one model is universally superior. Model performance depends on the type of fraud, dataset characteristics, and implementation environment.

4.4 Data Imbalance

One of the most important findings in the literature is the problem of data imbalance.

In many financial datasets, legitimate transactions greatly outnumber fraudulent transactions. As a result, a system could appear highly accurate while still failing to identify a significant number of fraudulent transactions.

Researchers have therefore developed techniques to address data imbalance. These include oversampling, undersampling, synthetic-data generation, and hybrid approaches.

The 2024 banking-fraud literature review found that data-balancing and preprocessing techniques can improve the performance of fraud-detection models.

4.5 False Positives

Another important issue is false positives.

If an AI system incorrectly identifies a legitimate transaction as fraudulent, the customer's transaction may be blocked or delayed.

A large number of false positives can create several problems:

- Customer dissatisfaction
- Additional investigation costs
- Increased workload for fraud analysts
- Delayed transactions
- Loss of customer trust

Therefore, the objective of a fraud-detection system should not simply be to identify as many suspicious transactions as possible. It must also distinguish legitimate activity from actual fraud. Research on explainable AI in finance emphasizes the importance of understanding model decisions, particularly when incorrect alerts can affect customers and financial institutions.

4.6 The Problem of Changing Fraud Techniques

Fraudsters continuously develop new techniques.

This creates a problem known as concept drift, where the patterns observed in historical data no longer accurately represent current fraudulent behavior.

For example, a model trained primarily on older types of payment fraud may not recognize a new type of digital fraud.

Recent reviews identify changing fraud patterns and concept drift as important challenges for AI-based financial fraud detection.

Therefore, AI systems must be continuously monitored and updated.

4.7 Explainability

One of the most important disadvantages of advanced AI systems is that their decisions may be difficult to explain.

A traditional rule might say:

"The transaction was flagged because it exceeded the predefined limit."

An advanced machine-learning model may instead identify a transaction based on hundreds of interacting variables.

This creates a problem for financial institutions because investigators may need to understand why a transaction was flagged.

Explainable AI attempts to address this problem by providing information about the factors that contributed to a model's decision. Recent research identifies explainability as an important requirement for trust, accountability, and regulatory compliance in financial AI systems.

4.8 Human Oversight

The evidence suggests that AI should not necessarily operate independently.

AI can automatically identify suspicious transactions, but human investigators can provide additional context that an algorithm may not have.

For example, an investigator may know that a customer is traveling internationally or has recently purchased an expensive item. The AI system may interpret this activity as unusual, while the investigator can determine whether there is a legitimate explanation.

Human oversight can therefore help reduce incorrect decisions and provide additional accountability.

4.9 Summary of Results

Table 3. Main Findings of the Research

Research Area	Finding
Large-scale processing	AI can analyze very large transaction datasets.
Pattern recognition	AI can identify complex relationships in transaction data.
Fraud detection	AI can improve the identification of suspicious transactions.
New fraud patterns	AI can assist with anomaly detection, but changing fraud remains a challenge.
False positives	AI can potentially reduce unnecessary alerts, but false positives remain a problem.
Data imbalance	Highly imbalanced datasets can affect model performance.
Explainability	Complex models may be difficult to interpret.
Human oversight	Human investigators remain important for reviewing alerts and decisions.
Adaptability	AI can be updated using new data, but continuous monitoring is necessary.

Overall, the results indicate that AI provides significant capabilities for fraud detection, but its effectiveness depends heavily on data quality, model selection, continuous monitoring, and human oversight.

Discussion and Conclusion:

This research examined whether artificial intelligence is really helpful in detecting financial fraud. The findings indicate that AI can provide significant benefits to fraud-detection systems. Machine-learning and deep-learning models can analyze large amounts of transaction data, identify complex patterns, detect unusual behavior, and assist financial institutions in monitoring transactions in real time. Research reviewed in this study shows that several AI techniques can perform strongly in fraud-detection applications. Models such as Random Forest, XGBoost, LightGBM, neural networks, and anomaly-detection systems have been used across different financial applications. However, AI is not a perfect solution.

One of the most important challenges is data imbalance. Fraudulent transactions are usually much less common than legitimate transactions, meaning that a model can appear accurate while still failing to detect some fraudulent activity.

Another challenge is that fraud changes over time. Fraudsters continuously develop new methods, meaning that AI systems must be updated and monitored to remain effective.

Explainability is another important issue. Some advanced AI models operate in ways that are difficult for humans to understand. This can create problems when banks need to explain why a customer's transaction was flagged or why a particular decision was made. Recent research emphasizes the importance of explainable AI, transparency, and human oversight in financial fraud detection.

The comparison with traditional fraud detection shows that AI offers advantages in processing large amounts of data, recognizing complex patterns, and adapting to changing behavior. Traditional rule-based systems, however, remain useful because they are relatively simple to understand and can provide clear explanations for their decisions.

Therefore, the evidence indicates that AI is genuinely helpful in detecting financial fraud, but its role should not be viewed as completely replacing traditional systems or human investigators.

A more effective approach is to combine AI with existing fraud-detection rules and human expertise. AI can monitor transactions and identify suspicious patterns, while traditional rules can handle known risks and human investigators can review complex or uncertain cases.

From a practical perspective, financial institutions should focus not only on model accuracy but also on false positives, explainability, data quality, privacy, security, and continuous monitoring.

Future research could examine how AI fraud-detection systems perform using real-time transaction data and how effectively they respond to new fraud techniques. Researchers could also investigate how explainable AI can improve the ability of fraud investigators to understand and verify AI-generated alerts.

In conclusion, AI has demonstrated meaningful potential in financial fraud detection. However, its effectiveness depends on how it is designed, trained, monitored, and integrated into the broader fraud-detection process. AI should therefore be considered a powerful tool within a broader fraud-prevention system rather than a completely independent solution. Finally, AI's use should not be limited to Fraud detection or even financial metrics, other non financial metrics such as sustainability, social responsibility and benefiting humanity should be an important part of the use of Artificial Intelligence (Kaspard et al., 2026; Kaspard et al., 2025).

References

- Athari, S. A., Saliba, C., Khalife, D., & Salameh-Ayanian, M. (2023). The role of country governance in achieving the banking sector's sustainability in vulnerable environments: New insight from emerging economies. *Sustainability*, 15(13), 10538.
- Athari, S. A., Sassine, M. E., Agyemang, E. T., Kirikkaleli, D., & Saliba, C. (2026). Nonlinear Dynamics of AI Investment and Economic Growth in Germany: Evidence from a NARDL Approach. *Economies*, 14(1), 31.
- Azoury, N., Subrahmanyam, S., & Sarkis, N. (2024). The Influence of a Data-Driven Culture on Product Development and Organizational Success through the Use of Business Analytics. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 15(2), 123-134.
- Chaanine, N., Mhanna, R. Y., Verdie, J. F., & Beainy, R. (2023). Leveraging business experience and knowledge to boost entrepreneurial achievement. *International Journal of Work Innovation*, 4(2), 104-115.
- Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, 12, 6. <https://doi.org/10.1186/s40537-024-01048-8>
- 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, 1130. <https://doi.org/10.1057/s41599-024-03606-0>
- Kaspard, J. A., Khalil, F. C., & Kamel, C. A. (2025). Factors contributing to non-financial performance of companies. In *Sustainable Economic Development: Utilizing Non-Financial Performance, Sustainability Reporting, and Corporate Governance* (pp. 413-442). Cham: Springer Nature Switzerland.
- Kaspard, J., Kamel, C., Khalil, F., & Beainy, R. (2026). Financial Performance, Risk, and Market Integration of Sustainability-Oriented Equity Indices: Implications for the Sustainability Transition (2010–2025). *Risks*, 14(5), 99.
- Khalife, D., Subrahmanyam, S., & Farah, A. (2024). A Sustainable Circular Business Model to Improve the Performance of Small and Medium-sized Enterprises Using Blockchain Technology. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 15(2), 240-250.
- Khalife, D., Yammine, J., Rahal, S., & Freiha, S. (2023). Pricing Asian and Barrier Options Using a Combined Heston Model and Monte Carlo Simulation Approach with Artificial Intelligence. *Mathematical Modelling of Engineering Problems*, 10(5), 1690.
- Khan, F. S., Mazhar, S. S., Mazhar, K., AlSaleh, D. A., & Mazhar, A. (2025). Model-agnostic explainable artificial intelligence methods in finance: A systematic review, recent developments, limitations, challenges and future directions. *Artificial Intelligence Review*, 58, 232. <https://doi.org/10.1007/s10462-025-11215-9>
- Mousavian, S., & Miah, S. J. (2025). Review of artificial intelligence-based applications for money laundering detection. *Intelligent Systems with Applications*, 27, 200572. <https://doi.org/10.1016/j.iswa.2025.200572>

- Saber, A. M., & Sassine, M. E. (2022). Reflections on internal control and internal audit roles for ensuring financial transparency toward Lebanese NGOs financial donors. *EuroMed Journal of Management*, 4(3), 186-198.
- Sawaya, C., Khalil, F. C., Jabbour Al Maalouf, N., & Kaspard, J. (2026). Revolutionizing audit practice in emerging economies: the role of Artificial Intelligence in enhancing the audit of consolidated financial statements. *Cogent Business & Management*, 13(1), 2625974.
- Yanto, Y., Lisah, L., & Tandra, R. (2024). The best machine learning model for fraud detection in banking sector: A systematic literature review. *ECo-Buss*, 7(2), 1361–1384.
<https://doi.org/10.32877/eb.v7i2.1474>
- Yeo, W. J., Van Der Heever, W., Mao, R., Cambria, E., Satapathy, R., & Mengaldo, G. (2025). A comprehensive review on financial explainable AI. *Artificial Intelligence Review*, 58, 189. <https://doi.org/10.1007/s10462-024-11077-7>
- Zafar, U., & Wu, F. (2026). Methodological challenges in explainable AI for fraud detection: A systematic literature review. *Artificial Intelligence Review*, 59, 115.
<https://doi.org/10.1007/s10462-026-11516-7>