Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 1, April 2026, pp. 272~282
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i1.pp272-282

Fraud detection in financial transactions: state of the art

Hamza Badri[1], Youssef Balouki[2], Fatima Guerouate[2]
[1]Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI), Mohammadia School of Engineers Mohammed V University, Rabat, Morocco
[2]Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI), Mohammed V University, Rabat, Morocco

Article Info

Article history:

Received Jul 2, 2025
Revised Jan 23, 2026
Accepted Feb 24, 2026

Keywords:

Anomaly detectio
Data mining
Deep learning
Financial transaction
Fraud detectio
Machine learnin

ABSTRACT

The surge in digital financial transactions, fueled by the proliferation of online banking, ecommerce, and emerging technologies, has brought significant oppor- tunities and equally critical vulnerabilities. Fraudulent activities have evolved in parallel, leveraging the complexity and global reach of digital systems to exploit weaknesses. This paper investigates the multifaceted nature of fraud in financial transactions, focusing on key types such as credit card fraud, money laundering, insurance fraud, and emerging threats in cryptocurrency systems. In this paper, we establish a state-of-the-art overview of fraud detection method- ologies, analyzing their strengths and limitations. Traditional rule-based ap- proaches are contrasted with modern machine learning (ML) models, hybrid frame- works, and the application of advanced technologies. The study highlights the critical role of systems capable of identifying complex fraud patterns while ad- dressing persistent challenges. By synthesizing findings from existing research and evaluating innovative methods, this paper provides actionable insights into enhancing the effectiveness and resilience of fraud detection systems.

Corresponding Author:

Hamza Badri
Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI)
Mohammed V University
Rabat, Morocco
Email: hamza_badri2@um5.ac.ma

1. INTRODUCTION

The way we handle money has been completely reshaped by digital services. Everyday tools like online banking, e-commerce, and mobile payments have made finance more accessible and efficient for everyone. However, this convenience has also created new vulnerabilities. As the volume of digital transactions explodes, financial institutions find themselves in a constant battle against increasingly sophisticated fraud.

Today's fraud is not about forged checks or simple card theft anymore. Criminals now exploit complex global payment systems, use anonymizing tech, and target new platforms like cryptocurrencies and decentralized finance (DeFi). The financial cost is staggering, reaching billions of dollars annually and climbing, as cybercriminals continuously refine their methods [1]. It's clear that traditional security measures, often based on fixed rules, are no longer enough to handle this dynamic threat.

The initial response to digital fraud was to build systems based on expert-defined rules, such as flagging all transactions over a certain amount. While useful for known attack patterns, these static systems fail against new or evolving schemes. This is why the field has shifted towards machine learning (ML) and deep learning (DL). Instead of relying on fixed rules, these models learn complex and subtle patterns directly

from massive datasets of transaction history. Recent developments, particularly with graph-based models that map fraud networks and ensemble methods that combine multiple detectors, have significantly improved performance.

However, in reviewing the current literature, we identified three critical gaps. First, most studies operate in silos, focusing on a single fraud type (like credit cards) or one detection technique, which prevents a clear comparison of what works best across different domains. Second, many papers chase incremental accuracy gains while ignoring crucial real-world challenges like computational cost, model interpretability for regulators, and the difficulty of deploying in real-time. Third, the risks tied to emerging technologies, such as those in blockchain systems or privacy-preserving frameworks, remain underexplored in existing surveys.

This paper directly addresses these gaps. We provide a comprehensive review that systematically compares traditional, ML, DL, and hybrid approaches across a wide range of fraud categories—from insurance and mortgage fraud to money laundering and crypto-related schemes. Our focus is on practical applicability, weighing the trade-offs between performance and real-world deployability. Ultimately, our goal is twofold. We aim not only to summarize the current state of research but also to critically analyze the strengths and weaknesses of today's methods. By highlighting open challenges and future directions, we hope to equip researchers and practitioners with the insights needed to build the next generation of robust, scalable, and truly adaptive fraud detection systems.

The main contributions of this paper can be summarized as follows: To achieve our goal, this paper is built around four core contributions. We begin by creating a clear and structured taxonomy to organize the sprawling landscape of financial fraud. This framework is designed to be practical, covering not only traditional domains like credit card and insurance fraud but also integrating the novel threats emerging from cryptocurrencies. Building on this classification, we then benchmark a wide range of detection methods against each other. Our analysis moves beyond simplistic accuracy metrics to offer a comparative view of traditional rules, ML, and DL models, weighing their trade-offs in terms of computational cost, interpretability, and real-world readiness. This practical focus naturally leads to our third contribution: a critical discussion of the persistent challenges that practitioners face daily. We dedicate specific attention to issues like severe data imbalance, concept drift (when fraud patterns change over time), and the immense pressure of real-time processing constraints and data privacy regulations. Finally, by synthesizing these findings, we identify the most significant research gaps and propose a roadmap for future innovation. We argue that the next generation of fraud detection systems will likely emerge from the integration of promising technologies like graph-based learning, federated learning, and blockchain analytics.

2. RELATED WORK AND FRAUD DETECTION TAXONOMY

2.1. Types of financial fraud

Fraud is not a monolithic problem; its methods are tailored to specific industries and objectives. The techniques used for insurance fraud, for example, are fundamentally different from those employed in money laundering or attacks against emerging cryptocurrency platforms. While new threats constantly appear, the sheer volume of digital payments ensures that credit card fraud remains one of the most persistent and widespread challenges.

To bring structure to this complex landscape, our analysis will be guided by the comprehensive classification framework proposed in [2]. This model organizes financial fraud into distinct categories—including credit card, money laundering, and loan-related schemes—which we will use as a foundation for our comparative analysis. The figure below provides a visual map of these primary fraud types, each of which requires a unique detection strategy. By understanding their underlying mechanisms, we can then evaluate which detection models are most effective for each specific case. To provide a structured overview of the financial fraud landscape, Figure 1 summarizes the main categories of financial fraud addressed in the literature, highlighting their diversity across different application domains.

2.1.1. Credit card fraud

The explosion of e-commerce and digital payments has made credit cards a primary target for fraud. As transaction volumes have surged [3], so have the opportunities for criminals. Fraudsters now employ a range of sophisticated techniques, from digital methods like phishing to physical ones like card skimming and the creation of highly convincing counterfeit cards [4]. These unauthorized activities result in significant financial losses for both consumers and banks, a problem made worse by the anonymity and global reach of online platforms, which complicates law enforcement efforts [5].

In response, financial institutions have turned to technology, deploying ML and AI systems to fight back. These models are designed to analyze vast streams of transaction data in real-time, identifying anomalous patterns that signal potential fraud before a transaction is even completed. However, this is not a

one-time fix. It's a continuous arms race. As detection systems become more advanced, so do the strategies of the fraudsters. This dynamic highlights the critical need for detection models that are not only accurate but also highly adaptive to the ever-evolving landscape of credit card fraud.

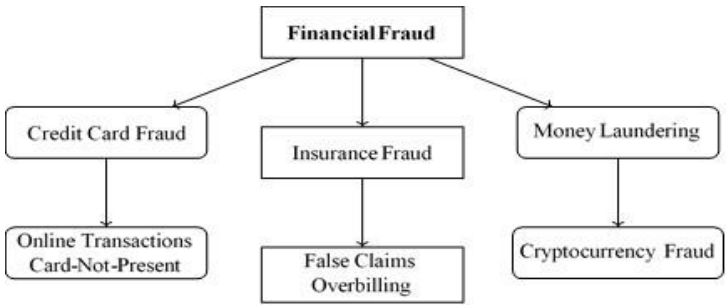

Figure 1. Taxonomy of major types of financial fraud

2.1.2. Insurance fraud

Unlike the high-volume, transactional nature of credit card fraud, insurance fraud encompasses a diverse set of schemes aimed at extracting illicit payments from an insurance policy. These schemes can be perpetrated by policyholders, agents, or organized rings at any point in the insurance lifecycle. The methods are highly context-specific: they can range from staging a car accident with exaggerated damage claims, to a medical provider billing for services never rendered, to a farmer artificially inflating crop losses after a natural disaster [6].

The primary challenge in combating insurance fraud is its sheer variety; a model trained to detect suspicious auto claims is useless for identifying fraudulent health services. Because a single detection strategy is insufficient, insurers are moving beyond simple rules. They are now deploying a combination of advanced data analytics and ML algorithms designed to spot anomalies across different business lines, often collaborating across borders to track complex international schemes.

2.1.3. Financial statement fraud

Shifting from high-volume external attacks, financial statement fraud represents a deliberate, internal manipulation of a company's perceived health. This form of fraud is not about single illicit transactions but about distorting the entire financial narrative. Executives might inflate revenues, hide liabilities, or alter asset valuations [7] with the specific goal of deceiving investors, securing favorable loans, or artificially boosting stock prices. The consequences can be catastrophic, leading to major market disruptions and devastating stakeholder losses.

Because this fraud is hidden within periodic reports rather than real-time data streams, detection relies on a different toolkit. It combines traditional forensic accounting and trend analysis with advanced ML algorithms trained to spot subtle anomalies and inconsistencies that a human auditor might miss. The challenge lies in identifying manipulations that are designed to look like normal business fluctuations, requiring a deep understanding of both accounting principles and the specific tactics used by fraudsters.

2.1.4. Money laundering

Unlike fraud that directly steals funds, money laundering is a secondary crime designed to legitimize the proceeds of other illegal activities, from drug trafficking to terrorism financing [8]. Its entire purpose is to erase the connection between the money and the crime. To do this, criminals typically follow a three-stage playbook. First, they place the illicit cash into the financial system, often through small deposits or legitimate-looking businesses. Next, they layer it by moving the funds through a complex web of transactions—often crossing multiple borders and involving shell corporations—with the sole aim of obscuring the original source. Finally, they integrate the "cleaned" money back into the legitimate economy through investments or large purchases.

This multi-stage process is precisely what makes detection so challenging. In response, global regulators have mandated robust anti-money laundering (AML) and know your customer (KYC) frameworks. KYC regulations are designed to disrupt the "placement" stage by verifying identities, while advanced AML transaction monitoring systems are built to untangle the complex patterns of the "layering" stage, aiming to protect the integrity of the financial system.

2.1.5. Mortgage fraud

Unlike the rapid-fire nature of payment fraud, mortgage fraud is a slower, more deliberate deception centered on the application process itself. It involves intentionally falsifying information—from inflating property values to providing fake income details—to secure a loan that the borrower would otherwise be denied [9]. While the immediate goal is to deceive a single lender, the collective impact of such actions can be far more damaging. Widespread mortgage fraud can distort property values, create housing bubbles, and lead to significant financial instability that affects entire communities. Consequently, countermeasures focus heavily on the verification stage, combining stricter due diligence with ML models designed to flag suspicious patterns in application data. To situate our work within this diverse landscape, we present a comparative analysis of recent literature in Table 1. The table maps out key existing surveys, highlighting their focus areas—from healthcare and credit card fraud to money laundering and cryptocurrency schemes. As the comparison illustrates, most studies concentrate on a single fraud type. This underscores the critical gap our comprehensive, cross-domain review aims to fill, providing a unified perspective that is currently lacking in the field.

2.1.6. Cryptocurrency fraud

The very features that make cryptocurrencies revolutionary—decentralization, pseudo-anonymity, and the absence of traditional financial intermediaries—also make them a fertile ground for a new generation of fraud. Criminals exploit the promise of high, rapid returns to lure investors into sophisticated schemes. These are not isolated incidents; organized fraudulent services like BTCQuick and CoinOpened have managed to extract millions of dollars from investors by leveraging the largely unregulated nature of the digital currency market.

This fraud manifests in diverse forms, from investment-based scams like Ponzi schemes, fake initial coin offerings (ICOs), and "pump-and-dump" manipulations, to direct theft through phishing attacks designed to steal users' private keys. The core challenge in combating these activities stems directly from the technology itself. The pseudo-anonymous and borderless nature of blockchain transactions makes it incredibly difficult to trace illicit funds and identify perpetrators, a problem compounded by the constantly evolving tactics of fraudsters. This has prompted a dual response: a push for clearer regulatory frameworks from authorities and a drive for stronger on-chain security measures from developers.

2.2. Traditional fraud detection techniques

Fraud detection in the financial sector involves a range of techniques aimed at identifying and prevent- ing fraudulent activities. As fraudulent behaviors continuously evolve, understanding the different detection methods and evaluating their effectiveness becomes crucial. This section explores the primary methods used to detect fraud, focusing on their advantages, limitations, and specific applications [10]–[12]. Additionally, we provide a detailed comparative analysis with previous reviews that have addressed the same topic. The following table summarizes the key characteristics explored in these studies, comparing them with our approach. The comparison criteria include the scope of topics covered, the methodologies employed, and the limitations identified [3], [8]. This comparative analysis highlights the innovative aspects and contributions of our work, building on existing literature and providing new insights [5], [13]. Traditional fraud detection techniques form the foundation of fraud detection systems, often relying on rule-based systems defined by domain experts, auditors, or regulatory bodies. These methods are essential for identifying known fraud patterns, but they face challenges when it comes to detecting novel or evolving fraudulent behaviors.

2.2.1. Rule-based systems

These systems operate based on predefined rules or thresholds that are established by experts or through historical data analysis. They are designed to flag suspicious activities by identifying patterns consistent with known fraud types. For example, they may trigger alerts for transactions exceeding a certain amount, or for unusual behaviors, such as frequent withdrawals from the same account within a short period. These thresholds are often set based on the experience and knowledge of fraud investigators, and they are generally effective in detecting fraud that follows well-known patterns [10], [11]. However, these systems may struggle when faced with sophisticated or new types of fraud, which do not fit existing patterns [4].

2.2.2. Statistical methods

Statistical-based methods represent one of the earliest approaches to fraud detection in financial transactions. These techniques rely on probabilistic models and statistical assumptions derived from historical transaction data to identify anomalous or suspicious behaviors. Commonly used models include logistic regression, Bayesian inference, Gaussian-based anomaly detection, and probability scoring techniques. The main advantage of statistical methods lies in their simplicity, interpretability, and low computational cost, making

them suitable for real-time fraud detection systems. However, their effectiveness is often limited when dealing with highly imbalanced datasets, evolving fraud patterns, and complex non-linear relationships, which has motivated the transition toward ML and DL-based approaches.

2.2.3. Expert systems

Manual and automated audits remain a critical method for detecting anomalies. In manual auditing, fraud investigators examine transaction records and business processes to identify potential fraudulent activities. Automated auditing systems use pre-defined algorithms to analyze historical data and flag discrepancies in business processes, transaction flows, and compliance with regulatory standards. Despite their importance, audit systems also have limitations, such as the potential for human error in manual audits and the inability of automated systems to detect more complex fraud schemes [3], [12].

2.3. ML-based approaches

ML-based approaches have been widely adopted for fraud detection due to their ability to learn complex patterns from historical transaction data. Unlike traditional rule-based and statistical methods, ML models can automatically adapt to evolving fraud behaviors by leveraging labeled datasets. Commonly used algorithms include decision trees [14], [15], support vector machines [16], [17], random forests [16], logistic regression, and k-nearest neighbors [18]. These techniques have demonstrated improved detection performance compared to traditional methods, particularly in scenarios involving large-scale and high- dimensional financial data. However, their effectiveness strongly depends on data quality, feature engineering, and the handling of class imbalance, which remain critical challenges in practical deployments [19]–[21].

2.4. DL-based approaches

DL-based approaches have gained significant attention in financial fraud detection due to their capacity to model complex, non-linear patterns in large-scale transaction data. Unlike traditional ML techniques, DL models can automatically learn hierarchical feature representations, reducing the reliance on manual feature engineering. Architectures such as artificial neural networks, convolutional neural networks [22], recurrent neural networks, long short-term memory networks [23], and autoencoders have been successfully applied to various fraud detection tasks, including credit card fraud and money laundering detection. Despite their strong detection capabilities, DL models often require large labeled datasets, high computational resources, and careful model tuning, which can limit their interpretability and real-time deployment in practical financial systems [24].

2.4. Hybrid and ensemble methods

Hybrid and ensemble-based fraud detection methods combine multiple detection techniques to improve robustness and overall performance. These approaches often integrate traditional rule-based systems with ML or DL models, or aggregate multiple classifiers using ensemble strategies such as bagging, boosting, and stacking. The motivation behind hybrid models is to leverage the strengths of different techniques while mitigating their individual limitations, particularly in handling imbalanced data and evolving fraud patterns. Although hybrid and ensemble methods generally achieve improved detection reliability, they may introduce additional system complexity and computational overhead, which can pose challenges for real-time financial applications [25].

3. REVIEW METHODOLOGY

This study adopts a structured and systematic review methodology to ensure transparency, rigor, and reproducibility. The objective is to provide a comprehensive analysis of fraud detection techniques in financial transactions by synthesizing high-quality and relevant research contributions.

3.1. Data sources and search strategy

The literature search was conducted using major scientific databases, including IEEE Xplore, Scopus, Web of Science (WoS), and ScienceDirect. These databases were selected due to their wide coverage of peer-reviewed journals and conference proceedings in computer science, artificial intelligence, and financial engineering. A systematic search strategy was applied using combinations of keywords such as “financial fraud detection”, “credit card fraud”, “money laundering detection”, “ML fraud detection”, “DL fraud detection”, and “anomaly detection in financial transactions”. Boolean operators (AND/OR) were used to refine the search and ensure comprehensive coverage of relevant studies. Figure 2 presents an overview of the literature search and study selection process used in this review, from database identification to the final selection of relevant studies.

3.2. Inclusion and exclusion criteria

To ensure the relevance and quality of the reviewed literature, explicit inclusion and exclusion criteria were defined.

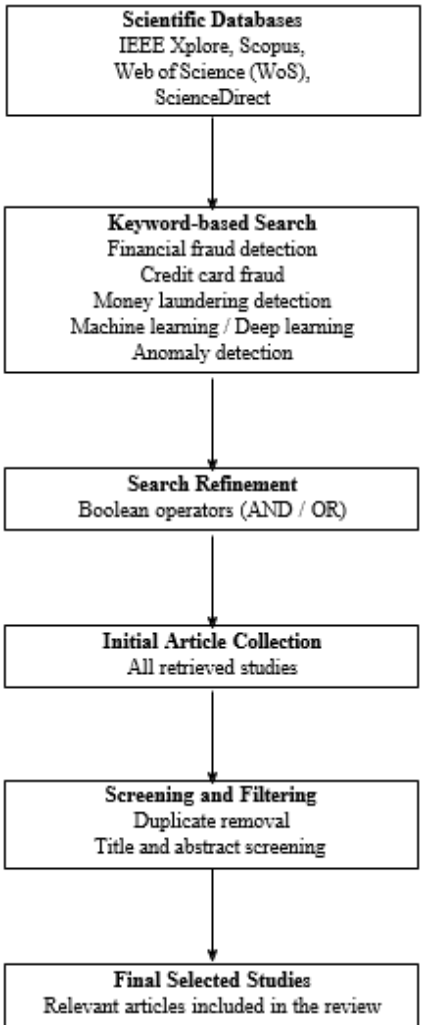

Figure 2. Literature search and study selection process

3.2.1. Inclusion criteria

The inclusion criteria were defined to ensure that only relevant, high-quality, and methodologically sound studies were considered in this review, as outlined below:

– Peer-reviewed journal articles and high-quality conference papers.
– Studies addressing fraud detection in financial transactions.
– Articles proposing or evaluating traditional, ML, DL, or hybrid detection approaches.
– Publications written in English.
– Studies published between 2010 and 2024.

3.2.2. Exclusion criteria

The exclusion criteria were established to filter out studies that do not meet the required quality standards or relevance to the scope of this research, as detailed below:

- Non-peer-reviewed articles, technical reports, theses, or white papers.
- Studies not directly related to financial fraud detection.
- Papers lacking sufficient methodological details or experimental validation.
- Duplicate publications across multiple databases.

3.3. Study selection and analysis

The study selection process was conducted in multiple stages. Initially, titles and abstracts were screened to remove irrelevant studies. Subsequently, full-text articles were assessed based on the predefined criteria. The selected studies were then categorized according to fraud type, detection methodology, data characteristics, and evaluation metrics. The final set of studies was analyzed to identify common trends, strengths, limitations, and research gaps. Comparative analysis was conducted considering performance, computational complexity, interpretability, scalability, and real-world applicability.

4. RESULTS AND DISCUSSION

4.1. Comparative analysis of fraud detection approaches

This section provides a comparative analysis of fraud detection approaches reported in the literature, focusing on their detection capabilities, computational requirements, and practical applicability [26]. Rather than presenting new experimental results, the discussion synthesizes findings from existing studies to highlight strengths, limitations, and trade-offs among traditional, ML, DL, and hybrid methods [27]–[29].

Table 1 summarizes representative studies on fraud detection in financial transactions reported in the literature, highlighting the application domains and types of fraud addressed. This synthesis illustrates the diversity of fraud scenarios, and research focuses considered across existing works. Table 2 provides a qualitative comparison between traditional rule-based approaches and modern ML and DL techniques based on commonly reported criteria in the literature, including accuracy, interpretability, adaptability, and scalability.

Table 1. Summary of representative studies on fraud detection in financial transactions

Article	Year	Fraud area	Type of fraud
[6]	2011	Healthcare insurance fraud	Insurance fraud
[10]	2011	All	General fraud detection
[11]	2012	Credit card and online auction	Credit card fraud
[30]	2013	Insurance fraud	Insurance fraud
[3]	2016	General fraud detection	Financial statement fraud
[4]	2018	Credit card fraud	Bank fraud: Credit card fraud
[5]	2018	Credit card fraud	Bank fraud: Credit card fraud
[13]	2024	Real-Time Online Banking Fraud Detection Model	Bank fraud
[7]	2023	Analysis of Banking Fraud Detection Methods	Bank fraud
[8]	2022	Credit card fraud detection model	Bank fraud: Credit card fraud

Table 2. Comparison between traditional and modern fraud detection techniques

Criteria	Traditional (Rule-based)	Modern (ML/DL)
Accuracy	Moderate, especially for known patterns	High, even for unknown patterns
Interpretability	High (clear rules)	Often low (black-box models)
Adaptability	Low (needs manual updates)	High (learns from new data)
Implementation Cost	Low (simple logic)	Medium to High (data, compute)
False Positives	Often high	Generally lower with proper tuning
Scalability	High	Varies (depends on infrastructure)

The comparison highlights a clear evolution from traditional rule-based systems toward data-driven ML and DL approaches [31]. While modern techniques generally offer higher detection capabilities and adaptability, traditional methods remain valuable due to their transparency, interpretability, and low implementation cost [32], [33]. These observations emphasize the importance of selecting fraud detection solutions based on application requirements and operational constraints [32], [34], [35].

4.2. Performance vs computational complexity trade-offs

Fraud detection systems must achieve a careful balance between detection performance and computational complexity, particularly in large-scale and real-time financial environments. While advanced ML and DL models often deliver superior detection accuracy, these gains are frequently accompanied by increased computational costs and resource requirements.

Traditional rule-based and statistical approaches are generally characterized by low computational complexity and fast execution times, making them suitable for real-time deployment and systems with strict latency constraints [36]. However, their limited ability to model complex and evolving fraud patterns often

results in reduced detection performance, especially when facing novel or sophisticated fraudulent behaviors [37].

ML techniques, such as decision trees, random forests, and support vector machines, offer a compromise between performance and complexity. These models are capable of capturing non-linear relationships in transactional data while maintaining reasonable computational efficiency [38]. Nevertheless, their performance can degrade when dealing with highly imbalanced datasets or rapidly changing fraud strategies, unless frequent retraining and feature engineering are applied [39].

DL models, including neural networks and hybrid architectures, demonstrate strong capabilities in detecting complex fraud patterns and subtle anomalies. Despite their high detection performance, these models typically require substantial computational resources, large volumes of labeled data, and longer training times. This complexity may limit their applicability in real-time or resource-constrained financial systems without specialized infrastructure.

Overall, the choice of fraud detection technique should be guided by operational constraints, including system scalability, real-time requirements, data availability, and computational resources. In practice, hybrid approaches that combine lightweight rule-based mechanisms with ML or DL models are increasingly adopted to balance performance and computational efficiency [40]- [42].

4.3. Interpretability and practical deployment considerations

Although detection performance is a key objective, interpretability and practical deployment remain critical factors in real-world fraud detection systems. In many financial institutions, fraud detection models are not only required to identify suspicious transactions but also to provide explanations that can be understood by analysts, auditors, and regulatory authorities [43].

Traditional rule-based systems are still widely used in operational environments due to their transparency and ease of interpretation. The decision logic behind these systems is explicit, which allows practitioners to easily trace why a transaction was flagged as fraudulent [44]. This level of interpretability is particularly important in regulated financial contexts, where accountability and compliance requirements are strict. However, the rigidity of predefined rules often limits their effectiveness in detecting emerging fraud patterns [45].

ML models offer improved flexibility and detection capability, but interpretability becomes more challenging as model complexity increases. While some models, such as decision trees or logistic regression, remain relatively interpretable, others, including ensemble methods, require additional tools to explain their decisions. In practice, this trade-off often leads institutions to favor models that provide an acceptable balance between predictive performance and explainability rather than purely optimizing accuracy [46], [47]. DL approaches further amplify this challenge. Despite their strong ability to capture complex transactional behaviors, these models are frequently criticized for their black-box nature. The lack of clear explanations can hinder trust and slow down adoption, especially in high-stakes financial decision-making. As a result, DL models are often deployed alongside post-hoc explanation techniques or combined with simpler models to improve transparency.

From a deployment perspective, practical constraints such as system integration, maintenance, and scalability also influence model selection. Fraud detection systems must operate reliably in real-time environments, handle large transaction volumes, and adapt to evolving fraud strategies. Consequently, many real-world systems adopt hybrid frameworks that integrate interpretable rules with data-driven models, allowing institutions to benefit from advanced detection capabilities while maintaining operational control and regulatory compliance.

4.4. Domain-specific challenges and observation

Despite significant advances in fraud detection techniques, several challenges remain unresolved and continue to limit the effectiveness of existing systems. One of the most persistent issues is the highly imbalanced nature of financial transaction data, where fraudulent activities represent only a small fraction of overall transactions. This imbalance often biases models toward majority classes, leading to missed fraud cases or an excessive number of false alerts [48].

Another major challenge is the dynamic and evolving behavior of fraudsters. Fraud patterns change rapidly as attackers adapt to detection mechanisms, rendering static models and fixed rules ineffective over time [48], [49]. This concept drift requires continuous model updates, frequent retraining, and constant monitoring, which can be costly and operationally complex for financial institutions.

Data quality and availability also pose important limitations. In many real-world scenarios, labeled fraud data is scarce, noisy, or delayed due to investigation processes [50]. Moreover, privacy regulations and data-sharing restrictions often limit access to comprehensive datasets, making it difficult to develop robust and generalizable models. These constraints are particularly problematic for data-hungry DL approaches. From an operational standpoint, the deployment of advanced fraud detection models raises additional

concerns. Integrating new models into legacy banking systems, ensuring real-time responsiveness, and maintaining system stability at scale remain non-trivial tasks. Furthermore, balancing detection accuracy with interpretability and regulatory compliance continues to be a delicate issue, especially in highly regulated financial environments.

Finally, there is a lack of standardized evaluation frameworks across studies. Many works rely on different datasets, metrics, and experimental settings, which complicates fair comparison and reproducibility. Addressing these open issues requires not only methodological improvements but also closer collaboration between researchers and industry practitioners to develop practical, transparent, and adaptable fraud detection solutions [51].

5. CONCLUSION

This paper presented a comprehensive state-of-the-art review of fraud detection techniques in financial transactions. By organizing existing studies into traditional, ML, DL, and hybrid approaches, the review highlighted the evolution of fraud detection systems and the growing complexity of modern financial fraud scenarios.

The analysis shows that while traditional rule-based and statistical methods remain relevant due to their transparency and low computational cost, they are often insufficient to cope with large-scale and rapidly evolving fraud patterns. ML and DL approaches provide improved detection capabilities by modeling complex transactional behaviors, yet they introduce challenges related to interpretability, computational complexity, and deployment in real-world financial environments. Hybrid and ensemble strategies have emerged as practical solutions, aiming to balance detection performance with operational constraints.

Beyond performance considerations, this review emphasized the importance of practical factors such as data quality, model explainability, regulatory compliance, and system scalability. These aspects play a crucial role in determining the real-world applicability of fraud detection models and often influence model selection more strongly than accuracy alone.

Future research should focus on developing adaptive and interpretable fraud detection systems capable of handling evolving fraud strategies and highly imbalanced data. Promising directions include the integration of explainable artificial intelligence techniques, the use of semi-supervised and unsupervised learning to reduce dependence on labeled data, and the design of standardized evaluation frameworks to improve reproducibility and comparability across studies. Strengthening collaboration between academia and industry will also be essential to bridge the gap between theoretical advances and operational deployment.

REFERENCES

[1] V. Jain, A. Balakrishnan, D. Beeram, M. Najana, and P. Chintale, "Leveraging artificial intelligence for enhancing regulatory compliance in the financial sector," *International Journal of Computer Trends and Technology*, vol. 72, no. 5, pp. 124–140, May 2024, doi: 10.14445/22312803/ijctt-v72i5p116.

[2] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Computer Science Review*, vol. 40, p. 100402, May 2021, doi: 10.1016/j.cosrev.2021.100402.

[3] A. Mousa, "Detecting financial fraud using data mining techniques: a decade review from 2004 to 2015," *Journal of Data Science*, vol. 14, no. 3, pp. 553–570, Aug. 2022, doi: 10.6339/jds.201607_14(3).0010.

[4] M. K., "Credit card fraud detection using data mining techniques," *International Journal of Advanced Computer Science and Applications*, vol. 9, pp. 45–52, 2018.

[5] R. R. Popat and J. Chaudhary, "A survey on credit card fraud detection using machine learning," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, May 2018, pp. 1120–1125, doi: 10.1109/icoei.2018.8553963.

[6] P. Travaille, *Electronic fraud detection in the us medicaid health care program*. University of Twente, The Netherand., 2011.

[7] A. Hanae, G. Youssef, and E. Saida, "Analysis of banking fraud detection methods through machine learning strategies in the era of digital transactions," in *2023 7th IEEE Congress on Information Science and Technology (CiSt)*, Dec. 2023, pp. 105–110, doi: 10.1109/cist56084.2023.10409974.

[8] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, "Developing a credit card fraud detection model using machine learning approaches," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022, doi: 10.14569/ijacsa.2022.0130350.

[9] C.-W. Lee, M.-W. Fu, C.-C. Wang, and M. I. Azis, "Evaluating machine learning algorithms for financial fraud detection: insights from Indonesia," *Mathematics*, vol. 13, no. 4, p. 600, Feb. 2025, doi: 10.3390/math13040600.

[10] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, Feb. 2011, doi: 10.1016/j.dss.2010.08.006.

[11] P. Richhariya and P. Singh, "A survey on financial fraud detection methodologies," *International journal of computer applications*, vol. 45, pp. 15–22, 2012.

[12] Q. Liu and M. Vasarhelyi, "Healthcare fraud detection: A survey and a clustering model incorporating geo-location information," *29th world continuous auditing and reporting symposium (29WCARS), Brisbane, Australia*, 2013.

[13] H. Abbassi, S. El Mendili, and Y. Gahi, "Real-time online banking fraud detection model by unsupervised learning fusion," *HighTech and Innovation Journal*, vol. 5, no. 1, pp. 185–199, Mar. 2024, doi: 10.28991/hij-2024-05-01-014.

[14] Y. Shiau and C. Chen, "Application of decision tree algorithm in detecting fraudulent insurance claims," *Computational Intelligence and Neuroscience*, pp. 1–12, 2016.
[15] M. Ullah, F. Bashir, and R. Ahmed, "Fraud detection using random forest algorithm in credit card trans- actions," *Computational Intelligence*, vol. 36, pp. 987–999, 2020.
[16] I. Bashar, A. Sahu, and S. Ghosh, "Fraud detection using machine learning algorithms: A review," *Journal of Computer Science*, vol. 16, pp. 25–37, 2020.
[17] Y. Zhuang and X. Tan, "An application of svm for credit card fraud detection," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 209–213, 2019.
[18] L. Xie, X. Chen, and Y. Zhang, "A novel anomaly detection approach for credit card fraud detection using machine learning," *International Journal of Computer Applications*, vol. 178, pp. 12–22, 2020.
[19] M. Jain and S. Sharma, "Anomaly detection using k-means clustering algorithm," *International Journal of Computer Science and Information Security*, vol. 15, no. 9, pp. 21–28, 2017.
[20] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 Eighth IEEE International Conference on Data Mining*, Dec. 2008, pp. 413–422, doi: 10.1109/icdm.2008.17.
[21] U. Khakurel and D. B. Rawat, "Real-time physical threat detection on edge data using online learning," *IEEE Consumer Electronics Magazine*, vol. 13, no. 1, pp. 72–78, Jan. 2024, doi: 10.1109/mce.2023.3256641.
[22] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2323, 1998, doi: 10.1109/5.726791.
[23] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.
[24] S. Liu, Y. Li, and S. Zhang, "Reinforcement learning for fraud detection," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 5, pp. 1234–1245, 2020.
[25] B. Liu, Y. Zhang, and H. Li, "Reinforcement learning and stacked ensemble for adaptive fraud detection," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 9, pp. 4121–4133, 2021.
[26] J. West, M. Bhattacharya, and R. Islam, "Intelligent financial fraud detection practices: an investigation," in *International Conference on Security and Privacy in Communication Networks*, Springer International Publishing, 2015, pp. 186–203.
[27] S. G. S. - and S. H. K. -, "Detecting financial fraud in the digital age: the AI and ML revolution," *International Journal For Multidisciplinary Research*, vol. 5, no. 5, Sep. 2023, doi: 10.36948/ijfmr.2023.v05i05.6139.
[28] H. Xu, K. Niu, T. Lu, and S. Li, "Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects," *Engineering Science & Technology Journal*, vol. 5, no. 8, pp. 2402–2426, Aug. 2024, doi: 10.51594/estj.v5i8.1363.
[29] W. C. Aaron, O. Irekponor, N. T. Aleke, L. Yeboah, and J. E. Joseph, "Machine learning techniques for enhancing security in financial technology systems," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 2805–2822, Oct. 2024, doi: 10.30574/ijsra.2024.13.1.1965.
[30] H. Sithic and T. Balasubramanian, "Survey of insurance fraud detection using data mining techniques," *arXiv preprint arXiv:1309.0806*, vol. 2013.
[31] Z. Xia and S. C. Saha, "FinGraphFL: financial graph-based federated learning for enhanced credit card fraud detection," *Mathematics*, vol. 13, no. 9, p. 1396, Apr. 2025, doi: 10.3390/math13091396.
[32] Z. Wang, "Artificial intelligence and machine learning in credit risk assessment: enhancing accuracy and ensuring fairness," *Open Journal of Social Sciences*, vol. 12, no. 11, pp. 19–34, 2024, doi: 10.4236/jss.2024.1211002.
[33] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," *arXiv (Cornell University)*, 2025. http://arxiv.org/abs/2502.00201.
[34] N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," *Electronics*, vol. 11, no. 4, p. 662, Feb. 2022, doi: 10.3390/electronics11040662.
[35] S. Showalter and Z. Wu, "Minimizing the societal cost of credit card fraud with limited and imbalanced data," *arXiv (Cornell University)*, 2019. https://arxiv.org/abs/1909.01486.
[36] E.-A. Mînăstireanu and G. Meşniţă, "Methods of handling unbalanced datasets in credit card fraud detection," *Brain. Broad Research in Artificial Intelligence And Neuroscience*, vol. 11, no. 1, pp. 131–143, Mar. 2020, doi: 10.18662/brain/11.1/19.
[37] K. R. Kerwin and N. D. Bastian, "Stacked generalizations in imbalanced fraud data sets using resampling methods," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 18, no. 3, pp. 175–192, Nov. 2020, doi: 10.1177/1548512920962219.
[38] C. Charitou, S. Dragic˘evic´, and A. S. d'Avila Garcez, "Synthetic data generation for fraud detection using gans," *arXiv (Cornell University)*, 2021. https://arxiv.org/abs/2109.12546.
[39] A. O. Ikudabo and P. Kumar, "AI-driven risk assessment and management in banking: balancing innovation and security," *International Journal of Research Publication and Reviews*, vol. 5, no. 10, pp. 3573–3588, Oct. 2024, doi: 10.55248/gengpi.5.1024.2926.
[40] Y. Yazici, "Approaches to fraud detection on credit card transactions using artificial intelligence methods," in *Computer Science & Information Technology*, Jul. 2020, pp. 235–244, doi: 10.5121/csit.2020.101018.
[41] H. Manek, N. Kataria, S. Jain, and C. Bhole, "Various methods for fraud transaction detection in credit cards," *Journal of Ubiquitous Systems and Pervasive Networks*, vol. 12, no. 1, pp. 25–30, Nov. 2019, doi: 10.5383/juspn.12.01.004.
[42] N. Fariha *et al.*, "Advanced fraud detection using machine learning models: enhancing financial transaction security," *International Journal of Accounting and Economics Studies*, vol. 12, no. 2, pp. 85–104, Jun. 2025, doi: 10.14419/c73kcb17.
[43] 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, May 2021, doi: 10.1016/j.ins.2019.05.042.
[44] C. C. Lee and J. W. Yoon, "A data mining approach using transaction patterns for card fraud detection," *arXiv (Cornell University)*, 2013. https://arxiv.org/abs/1306.5547.
[45] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing credit card fraud detection: an ensemble machine learning approach," *Big Data and Cognitive Computing*, vol. 8, no. 1, p. 6, Jan. 2024, doi: 10.3390/bdcc8010006.
[46] R. Q. Majumder, "A review of anomaly identification in finance frauds using machine learning systems," *SSRN Electronic Journal*, 2025, doi: 10.2139/ssrn.5267287.
[47] M. Binsawad, "Enhanced financial fraud detection using an adaptive voted perceptron model with optimized learning and error reduction," *Electronics*, vol. 14, no. 9, p. 1875, May 2025, doi: 10.3390/electronics14091875.
[48] E. Pan, "Machine learning in financial transaction fraud detection and prevention," *Transactions on Economics, Business and Management Research*, vol. 5, pp. 243–249, Mar. 2024, doi: 10.62051/16r3aa10.

[49] S. Verma and J. Dhar, "Credit card fraud detection: A deep learning approach," *arXiv (Cornell University)*, 2024. http://arxiv.org/abs/2409.13406.
[50] A. C. P. Malik, "Credit risk assessment and fraud detection in financial transactions using machine learning," *Deleted Journal*, vol. 20, pp. 2061–2069, 2024, doi: 10.52783/jes.1807.
[51] Y. Abakarim, M. Lahby, and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning," in *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications*, Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.

BIOGRAPHIES OF AUTHORS

Hamza Badri is a researcher affiliated with the Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI), Mohammadia School of Engineers, Mohammed V University in Rabat, Morocco. His research interests include systems analysis, information processing, and industrial management, with a focus on developing innovative approaches to address complex engineering problems. He can be contacted at email: h.badri.doc@uhp.ac.ma.

Youssef Balouki is a member of the Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI), Mohammed V University in Rabat, Morocco. His work primarily focuses on information processing, intelligent systems, and optimization techniques applied to industrial and engineering domains. He can be contacted at email: balouki.youssef@gmail.com.

Fatima Guerouate is a researcher at the Laboratory for Systems Analysis, Information Processing and Industrial Management (LASTIMI), Mohammed V University in Rabat, Morocco. Her research interests encompass systems modeling, data analysis, and advanced computational methods for improving decision-making processes in industrial environments.