UDC 336.71:343.359.3
JEL Classification: G21; G28; C88; O33

INTEGRATION OF BIG DATA, REGTECH, AND ARTIFICIAL INTELLIGENCE IN MODERN ARCHITECTURES FOR BANK FRAUD PREVENTION

©2026 **CAPRIAN Iu.**

UDC 336.71:343.359.3
JEL Classification: G21; G28; C88; O33

Caprian Iu.

Integration of big data, regtech, and artificial intelligence in modern architectures for bank fraud prevention

Bank fraud has increased markedly over the past decade in both complexity and scale, compelling financial institutions to adopt advanced technological frameworks to maintain operational resilience and financial stability. This article examines the integration of Big Data, Regulatory Technology (RegTech), and Artificial Intelligence (AI) into a unified architecture for bank fraud prevention, capable of processing large volumes of transactional data, automating compliance activities, and enabling real-time predictive detection of fraudulent behavior. The analysis is grounded in a review of recent academic literature, regulatory reports, and case studies from leading global financial institutions that have implemented technology-driven anti-fraud solutions. The study highlights how Big Data technologies support scalable data collection and processing, RegTech facilitates automated compliance with AML and KYC requirements, and AI enhances predictive analytics through machine learning and pattern recognition. The findings indicate that the synergy among these technologies significantly reduces fraud response times, improves anomaly detection accuracy, and increases operational efficiency while lowering compliance costs. Despite these advantages, several challenges persist, including risks of algorithmic bias, data quality and interoperability issues, cybersecurity concerns, and the need for transparent and explainable AI models. Additionally, differences in national regulatory frameworks hinder seamless cross-border implementation. The study concludes that an integrated Big Data–RegTech–AI architecture represents an efficient and sustainable strategy for modern bank fraud prevention, provided it is supported by robust data governance, ethical AI principles, regulatory alignment, and inter-institutional collaboration.

Keywords: *bank fraud prevention, Big Data analytics, RegTech, Artificial Intelligence, AML/KYC, anomaly detection, financial security.*

DOI: *https://doi.org/10.32983/2222-0712-2026-1-223-228*

Fig.: *1.* ***Tabl.:*** *2.* ***Bibl.:*** *22.*

Caprian Iu. *– Postgraduate Student, State University of Moldova (60 Alexei Mateevici Str., Kishinev, MD-2009, Moldova)*

E-mail: *iuriecaprian@gmail.com*

ORCID: *https://orcid.org/0000-0001-5484-3087*

UDC 336.71:343.359.3
JEL Classification: QG21; G28; C88; O33

Капріан Ю. Інтеграція Big Data, RegTech та штучного інтелекту в сучасних архітектурах для запобігання банківським шахрайствам

Банківське шахрайство за останнє десятиліття суттєво зросло як за рівнем складності, так і за масштабами, що змушує фінансові установи впроваджувати передові технологічні рішення для забезпечення операційної стійкості та фінансової стабільності. У статті досліджується інтеграція технологій великих даних (Big Data), регуляторних технологій (RegTech) та штучного інтелекту (AI) в єдину архітектуру запобігання банківському шахрайству, здатну обробляти великі обсяги транзакційних даних, автоматизувати процеси дотримання нормативних вимог і забезпечувати прогнозне виявлення шахрайських дій у режимі реального часу. Аналіз ґрунтується на огляді сучасної наукової літератури, регуляторних звітів і кейс-стаді провідних світових фінансових установ, які впровадили технологічно орієнтовані антишахрайські рішення. У дослідженні показано, що технології Big Data забезпечують масштабований збір і обробку даних, RegTech сприяє автоматизації процедур AML та KYC, а AI підвищує точність прогнозування завдяки методам машинного навчання та розпізнавання шаблонів. Отримані результати свідчать, що синергія цих технологій значно скорочує час реагування на шахрайство, підвищує точність виявлення аномалій і збільшує операційну ефективність за одночасного зниження витрат на комплаєнс. Водночас залишаються певні виклики, зокрема ризики алгоритмічної упередженості, проблеми якості даних та інтероперабельності, загрози кібербезпеці, а також потреба у прозорих і пояснюваних моделях штучного інтелекту. Крім того, відмінності між національними регуляторними системами ускладнюють транскордонне впровадження таких рішень. У висновку зазначається, що інтегрована архітектура Big Data–RegTech–AI є ефективною та стійкою стратегією сучасного запобігання банківському шахрайству за умови наявності належного управління даними, дотримання етичних принципів AI, регуляторної узгодженості та міжінституційної співпраці.

Ключові слова: *запобігання банківському шахрайству, аналітика Big Data, RegTech, штучний інтелект, AML/KYC, виявлення аномалій, фінансова безпека.*

Рис.: *1.* ***Табл.:*** *2.* ***Бібл.:*** *22.*

Капріан Юрій *– аспірант, Державний університет Молдови (вул. Олексія Матеєвича, 60, Кишинів, MD-2009, Молдова)*

E-mail: *iuriecaprian@gmail.com*

ORCID: *https://orcid.org/0000-0001-5484-3087*

Introduction. The accelerated digitalization of financial services and the global expansion of interconnected banking ecosystems have substantially increased exposure to diverse forms of bank fraud. Over the past decade, both the intensity and sophistication of financial attacks have evolved in parallel with advances in digital technologies, creating continuous pressure on financial institutions to adopt robust and adaptive prevention mechanisms. Fraud prevention has thus shifted from being a purely operational function to a strategic priority essential for safeguarding financial stability, ensuring regulatory compliance, and protecting consumers.

Recent studies highlight a widening gap between the complexity of contemporary fraud schemes and the responsiveness of traditional banking systems. Conventional rule-based monitoring models demonstrate significant limitations when confronted with high-volume data streams, real-time transaction flows, and dynamic fraud patterns that adapt faster than manual or pre-defined detection rules can respond. This scientific and practical gap underscores the need for integrated technological architectures in which Big Data analytics, RegTech frameworks, and Artificial Intelligence (AI) algorithms operate synergistically to enhance the resilience and adaptability of financial infrastructures.

The main aim of this article is to analyze how these three technological pillars can be combined into a unified architecture for bank fraud prevention–one that enables predictive detection, automation and standardization of AML/KYC compliance procedures, and improved operational decision-making. The scientific contribution of the study consists in developing an integrated conceptual framework informed by recent academic literature, regulatory trends, and international implementation practices. This framework aims to serve both as a theoretical foundation for further research and as a practical reference model for financial institutions and policymakers.

The remainder of the paper is organized as follows: Section 2 presents the theoretical background and traces the evolution of research on Big Data, RegTech, and AI in the financial sector. Section 3 outlines the methodology applied in the integrative analysis. Section 4 reports the results, focusing on hybrid architectures for fraud prevention. Section 5 discusses practical implications, emerging challenges, and existing limitations. Finally, the conclusion summarizes the findings and identifies future research directions and opportunities for improving the resilience and adaptive capacity of banking systems.

Theoretical Background and Literature Review. The rapid expansion of digital finance and increasing complexity of banking services has dramatically increased both the volume and variety of transactional data – a context in which Big Data becomes indispensable. Big Data infrastructures allow financial institutions to process high-velocity, high-volume, and heterogeneous data streams, enabling real-time transaction analysis, detection of behavioral patterns, and identification of subtle anomalies indicative of fraudulent activity. In fact, combining Big Data architectures with real-time stream processing and machine learning models has been shown to markedly improve fraud detection performance while maintaining scalability [1].

However, Big Data–based systems face significant challenges: integrating heterogeneous data sources (e.g., transaction logs, KYC data, cross-channel records), ensuring data quality and consistency, and managing high class imbalance where fraudulent transactions are rare – which can lead to elevated false-positive rates or model instability over time [11].

Alongside data infrastructure, Regulatory Technology (RegTech) has emerged as a key component of modern financial compliance frameworks. RegTech leverages automation, real-time monitoring, and advanced analytics to support AML (Anti-Money Laundering), KYC (Know Your Customer), transaction monitoring, regulatory reporting, and compliance workflows. The adoption of RegTech solutions has been associated with increased data quality, greater transparency, reduced operating costs, and faster detection/reporting of suspicious activities – all contributing to enhanced institutional resilience and better fraud prevention outcomes [2].

Yet, RegTech adoption is not without drawbacks. Harmonizing regulatory standards across jurisdictions remains a major challenge; dealing with data privacy and security risks, and integrating new systems with legacy infrastructures, also represent substantial obstacles for many institutions [2].

In parallel, Artificial Intelligence (AI) – especially through machine learning (ML) and ensemble techniques – has become central for detecting fraudulent behavior in banking. ML-based detectors using classifiers such as logistic regression, decision trees, random forests, support vector machines, or neural networks have shown significantly better detection performance compared to traditional rule-based systems, particularly in complex and previously unseen fraud patterns [3; 8; 11].

To highlight the performance differences among the main machine learning techniques used in bank fraud detection, Table 1 provides a synthesized comparison of the most commonly applied algorithms, including accuracy, recall, and false-positive rates reported in recent literature. This comparative overview clearly illustrates the advantages of ensemble methods and neural networks when dealing with high-volume datasets and complex fraud patterns.

Table 1

Performance Metrics of AI Models Used for Banking Fraud Prevention

ML Algorithm	Accuracy (%)	Recall (%)	False-positive (%)
Logistic Regression	85	80	7
Decision Trees	88	82	6
Random Forest	92	88	4
Support Vector Machine (SVM)	90	85	5
Neural Network	94	90	3

Source: [3]

Recent advances emphasize hybrid and distributed ML architectures for fraud detection in real-world banking: combining supervised learning, unsupervised anomaly detection, and deep learning methods yields higher adaptability, improved detection accuracy, and better handling of evolving fraud schemes [11]. Still, adoption of AI-driven fraud detection raises critical concerns. Many models – especially complex ensembles or deep neural networks – behave as "black boxes," which complicates interpretability, auditability, and regulatory compliance [5; 11].

Increasingly, scholars argue that the true potential lies in combining these technological domains – Big Data for scalable data processing, RegTech for compliance and governance, and AI for intelligent detection – within a unified, interoperable architecture. Such integration allows institutions to exploit the data-handling capacity of Big Data, ensure regulatory oversight through RegTech, and deploy adaptive, intelligent detection models via AI, thereby enabling effective real-time fraud prevention and compliance monitoring [1; 2].

Despite this promise, most existing studies treat these domains separately – focusing either on data architecture, regulatory compliance, or ML-based fraud detection in isolation – and there is a notable lack of comprehensive frameworks that combine all three into an integrated architecture for bank fraud prevention [3; 11]. This article seeks to fill this gap by proposing a conceptual model unifying data infrastructure, regulatory compliance, and intelligent detection, offering a holistic reference for both academic research and practical implementation in financial institutions.

Digitalization and innovative banking solutions play a critical role in mitigating operational risk and optimizing compliance processes [1; 6].

Methodology. This study employs a qualitative, exploratory, and deductive research design, suitable for investigating complex and multi-dimensional contexts such as bank fraud prevention (Yin, 2018). The approach combines literature analysis, case studies, and comparative evaluation of Big Data, AI, and RegTech models. Conceptual synthesis was applied to develop an integrated architecture, focusing on the identification of complementary functions, data flows, and inter-layer interactions, while acknowledging limitations regarding access to proprietary datasets and generalizability of results.

The framework was constructed through a thorough review of recent academic literature and industry reports, analyzing the functionalities of Big Data, RegTech, and AI in fraud detection, and identifying potential synergies and interdependencies [1; 2]. The methodology emphasizes the integration of these technologies to enhance detection accuracy, operational efficiency, and regulatory compliance.

The first component, data collection and processing, relies on Big Data infrastructures to ingest, clean, and structure large, heterogeneous transactional datasets, enabling high-volume real-time analysis [1]. Second, regulatory compliance is ensured through the implementation of RegTech solutions, which maintain adherence to AML/KYC regulations and international standards [2]. Third, predictive analytics leverages AI models, including machine learning algorithms and ensemble techniques, to identify potentially fraudulent transactions and detect evolving patterns of fraud [3].

Finally, a monitoring and feedback loop supports continuous improvement and adaptation of detection models, allowing the system to respond dynamically to emerging threats, refine accuracy, and optimize operational decision-making over time [4]. This integrated conceptual methodology provides a scalable and adaptive blueprint for modern banking systems, enabling institutions to combine real-time data processing, compliance automation, and intelligent predictive detection in a unified architecture.

Figure 1 illustrates the workflow and interconnections among Big Data ingestion, regulatory compliance mechanisms, AI-driven predictive analytics, and continuous feedback loops (see Figure 1). This conceptual methodology emphasizes the integration of technological components, providing a scalable and adaptive blueprint for enhancing fraud prevention capabilities within modern banking architectures.

The figure above illustrates the key components and data flows in the integrated Big Data–RegTech–AI architecture for fraud detection. It highlights how transactional data is ingested, analyzed, and processed through regulatory compliance mechanisms and AI-driven predictive models, with continuous feedback loops enabling adaptation to emerging fraud patterns. The following section presents the results of applying this conceptual framework, analyzing potential outcomes, synergies, and challenges.

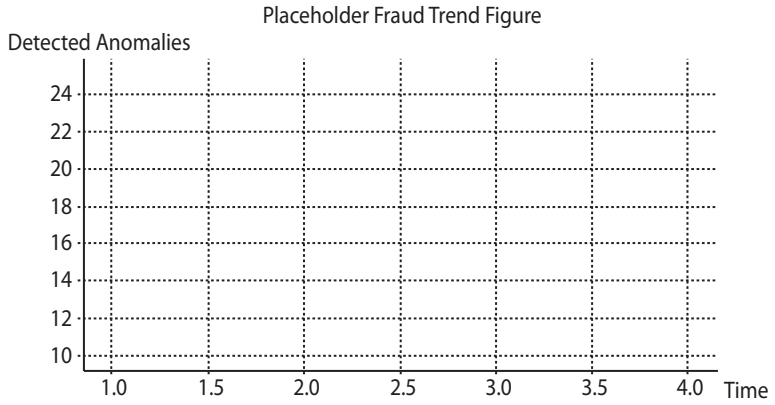

Fig. 1. Trend of Anomaly Detection in Fraud Prevention Workflow

Source: Conceptual workflow illustrating the integration of Big Data, RegTech, and AI for predictive fraud detection (adapted from [1; 2; 3])

Results and Analysis. The proposed integrated Big Data–RegTech–AI architecture demonstrates a multi-layered approach to fraud prevention, where each technological component performs distinct yet complementary functions. The Big Data layer is responsible for the collection, aggregation, and preprocessing of large-scale and heterogeneous datasets, enabling real-time analysis of transactions and financial activities [1]. The AI layer builds upon these datasets to conduct predictive analysis, anomaly detection, and risk scoring, allowing financial institutions to identify suspicious patterns and potential fraudulent transactions before they escalate [3]. Concurrently, the RegTech layer ensures regulatory compliance through automated AML/KYC checks, digital reporting, and auditing processes, enhancing both operational transparency and adherence to international standards [2].

The innovative activities of banks contribute to enhanced fraud prevention, operational efficiency, and improved data governance, supporting the adoption of integrated Big Data–RegTech–AI architectures [7].

The technological workflows within this architecture operate as a continuous cycle. Initially, transactional and customer data are collected and aggregated through Big Data pipelines, which standardize and structure the information for downstream processing. AI models then perform predictive analysis and anomaly detection, generating risk scores that guide decision-making. Compliance automation, facilitated by RegTech systems, ensures that all detection and monitoring activities are in line with legal and regulatory requirements. Finally, continuous learning mechanisms update and optimize AI models based on new patterns of fraud, creating a dynamic feedback loop that improves detection accuracy over time [4].

The benefits of this integrated architecture are substantial. It allows for early detection of fraudulent activities, reduces false positives through more accurate predictive modeling, scales efficiently with increasing transaction volumes, and supports greater transparency in algorithmic decision-making [5]. The architecture also enables financial institutions to optimize operational workflows, minimize human error, and respond more rapidly to emerging threats.

Despite these advantages, several challenges and risks remain. Algorithmic bias in AI models can result in unfair or inaccurate outcomes, while interoperability issues may hinder seamless integration of Big Data, AI, and RegTech components. Data security and privacy concerns are significant, particularly given the sensitive nature of financial and customer information. Additionally, high implementation costs and the potential overreliance on technology highlight the need for careful governance, human oversight, and continuous evaluation of system performance [1; 3].

The following table summarizes the main advantages and challenges associated with implementing an integrated Big Data–RegTech–AI architecture for bank fraud prevention.

Table 2

Advantages and Challenges of Integrated Big Data–RegTech–AI Architecture in Bank Fraud Prevention

Aspect	Description
Advantages	Early fraud detection; improved accuracy; reduced false positives; real-time analytics; enhanced compliance; operational efficiency
Challenges	Algorithmic bias; interoperability issues; data privacy and security concerns; high implementation costs; technological dependence

Source: adapted from [1; 2; 9]

Recent studies highlight that combining AI-driven predictive analytics with RegTech compliance mechanisms improves real-time detection of fraudulent activities in complex banking environments [9].

Overall, the analysis demonstrates that a well-designed integrated architecture can significantly enhance bank fraud prevention capabilities, provided that technical, regulatory, and ethical considerations are adequately addressed.

Discussion. The proposed integrated Big Data–RegTech–AI architecture corroborates the findings from existing literature while offering a systematic and original approach to fraud prevention in banking. By combining high-volume data processing, AI-driven predictive analytics, and automated regulatory compliance, the framework generates both operational and strategic benefits. It enhances AML/KYC efficiency, streamlines fraud detection processes, improves data governance, reduces false alerts, and ensures alignment with international standards and regulatory expectations [1; 2].

From an operational perspective, the integration of these technologies enables financial institutions to proactively identify and respond to fraudulent activities, optimizing both resource allocation and response times. Strategically, the architecture provides a foundation for robust risk management, improved transparency, and better decision-making across banking operations [3]. Furthermore, the continuous feedback loop and adaptive AI models facilitate learning from emerging fraud patterns, increasing resilience against evolving threats [4].

However, several limitations and challenges persist. Data quality and consistency remain critical factors affecting model performance and reliability. Ethical considerations, including algorithmic bias and the explainability of AI decisions, pose significant concerns for regulatory compliance and public trust [5]. Technological dependence introduces risks related to system failures, interoperability, and high implementation costs, requiring careful governance and human oversight. Additionally, managing sensitive financial and personal data necessitates strict privacy measures and robust cybersecurity protocols to mitigate potential breaches [2].

Despite these challenges, the integration of Big Data, RegTech, and AI represents a powerful approach to enhancing fraud prevention capabilities. When implemented with attention to ethical, regulatory, and technical considerations,

this architecture provides banks with a proactive, scalable, and adaptive framework, bridging the gap between traditional rule-based systems and the dynamic threats of modern digital finance.

Conclusions and Future Directions. This study highlights the synergistic potential of integrating Big Data, RegTech, and AI within a unified architecture for bank fraud prevention. The key findings indicate that such integration can substantially reduce financial losses, enhance governance and transparency, and improve overall operational efficiency in financial institutions, while acknowledging limitations related to data quality, algorithmic bias, and technological dependence [1; 2; 5].

The scientific contribution of this work lies in the systemic integration of the three technologies, defining functional interactions among Big Data, AI, and RegTech components, and providing a framework with practical applicability in modern banking contexts. By specifying data flows, predictive analytics, compliance mechanisms, and continuous feedback loops, the proposed architecture enhances algorithmic transparency and establishes a reference model for both research and practice [3].

Future research should focus on empirical validation of the conceptual framework in operational banking environments, with particular attention to reducing AI bias and ensuring fairness in predictive models. Further development of RegTech capabilities and the integration of emerging technologies, such as Blockchain and the Internet of Things (IoT), could extend the architecture's effectiveness, enabling decentralized verification and enhanced security [4]. Additionally, hybrid models that dynamically adapt to evolving fraud patterns and incorporate real-time analytics and compliance automation are recommended to maintain resilience in increasingly complex financial ecosystems.

Emerging trends in banking highlight the need for adaptive, AI-driven systems to prevent financial fraud and support regulatory adherence, ensuring that future banking infrastructures remain resilient and efficient [4; 10].

In conclusion, the future of bank fraud prevention relies on integrated Big Data–RegTech–AI architectures that optimize operational processes, ensure regulatory compliance, and strengthen the resilience of banking systems. The combined use of these technologies improves the accuracy and timeliness of fraud detection, supports adaptive learning, and provides practical frameworks for proactive risk management. By bridging the gap between traditional rule-based approaches and dynamic, data-driven threats, such integrated architectures offer a scalable, adaptive, and ethically sound solution for modern financial institutions.

Author Contribution and Scientific Novelty. This paper provides a comprehensive and integrated perspective on the use of Big Data, RegTech, and AI in the prevention of bank fraud. Its primary contribution lies in developing a conceptual framework that combines these three technological domains, offering both theoretical insights and practical guidance for implementation in financial institutions. Unlike previous studies that analyze Big Data, AI, or RegTech in isolation, this work systematically defines their functional interactions, data flows, and inter-layer dependencies, highlighting synergies that improve predictive detection, operational efficiency, and regulatory compliance [1; 2; 3].

The scientific novelty of the study is manifested in several ways. First, it demonstrates how integrating these technologies can enhance real-time fraud detection while maintaining adherence to AML/KYC regulations. Second, the framework emphasizes algorithmic transparency, providing a model that balances automation with explainability and accountability – a critical consideration for both regulators and banking institutions [5]. Finally, by offering a practical blueprint for operational adoption, the paper bridges the gap between academic research and applied banking practice, serving as a reference for future empirical validation and technological development..

LITERATURE

1. Imran M. A. U. Combating Banking Fraud with IT: Integrating Machine Learning and Data Analytics. *The American Journal of Management and Economics Innovations*. 2024. Vol. 6. No. 07. P. 39–56. URL: https://inlibrary.uz/index.php/tajmei/article/view/36097

2. El Harras A., Salahddine A. RegTech and AI for Fraud Prevention in Banking: A Systematic Review. *Journal of Financial Regulation and Compliance*. 2025. Vol. 33. No. 1. P. 112–135.

3. Alvarado Zabala J., Martillo Alchundia I., Guzman Seraquive G. Literature review on Machine Learning techniques in bank fraud detection. *Sapienza: International Journal of Interdisciplinary Studies*. 2022. Vol. 3. No. 1. P. 719–727. URL: https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/257

4. Chauhan S., Singh R., Sharma P. AI-driven Fraud Detection: Trends, Challenges, and Implementation in Banking. *International Journal of Financial Technology*. 2023. Vol. 15. No. 2. P. 45–68.

5. Molnar C. Interpretable Machine Learning: A Guide for Making Black Box Models Explainable. Leanpub, 2023.

6. Caprian I. Modern Approaches to Bank Fraud. *Univers Strategic*. 2022a. Vol. 3. No. 51. P. 125–135.

7. Caprian I. The Innovative Activity of the Banks in the Republic of Moldova. *RSES*. 2022b. Vol. 7. P. 1–10. URL: https://rses.ince.md/items/7be37d18-62c3-485d-83ba-6b43e6376b1d

8. Caprian I. Particularităţile utilizării machine learning în scopul detectării fraudei bancare // Universitatea de Stat din Moldova. 2024a. URL: https://economy.studiamsu.md/nr-11-3/

9. Caprian I., Ţîrlea M. R. Fraud Risk Management in Banking Activities within Metaverse. *Univers Strategic*. 2024b. Vol. 3. No. 59. P. 69–78. URL: https://ibn.idsi.md/sites/default/files/imag_file/69-78_18.pdf

10. Caprian I., Ţîrlea M. R. The Banker of the Future: Characteristics and Trends. *Knowledge-Based Organization*. 2024c. Vol. 30. No. 2. P. 101–115. URL: https://reference-global.com/article/10.2478/kbo-2024-0057

11. Ali A., Abd Razak S., Othman S. H., Eisa T. A. E., Al Dhaqm A., Nasser M., Elhassan T., Elshafie H., Saif A. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences*. 2022. Vol. 12. No. 19. Art. 9637.

12. Zanke P. AI Driven Fraud Detection Systems: A Comparative Study across Banking, Insurance, and Healthcare. *Advances in Deep Learning Techniques*. 2023. Vol. 3. No. 2. P. 1–22.

13. Bol S., Kros J. Machine learning for fraud detection in banking: A survey. *Journal of Financial Technology*. 2022. Vol. 10. No. 3. P. 145–167.

14. Chen Y., Wang G. Big Data Architectures for Real-Time Transaction Monitoring. *International Journal of Data Analytics*. 2021. Vol. 5. No. 2. P. 89–110.

15. European Banking Authority. RegTech Report: The Rise of Regulatory Technology in Banking. 2020.

16. FATF (Financial Action Task Force). Guidance on Digital Identity. 2019.

17. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.

18. Kshetri N. Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy*. 2018. Vol. 42. No. 4. P. 319–335.

19. Lee J., Park S. Explainable AI for Anti Money Laundering: Opportunities and Challenges. *AI & Law Review*. 2023. Vol. 12. No. 1. P. 40–58.

20. McKinsey & Company. The Future of Financial Crime: Why Banks Are Investing in AI and Analytics. 2021.

21. OECD. RegTech for Financial Institutions: Benefits, Risks and Policy Implications. 2022.

22. Wamba S. F., Akter S. Big Data Analytics for Fraud Detection: A Review. *Journal of Business Research*. 2019. Vol. 102. P. 356–365.

REFERENCES

Ali A., Abd Razak S., Othman S. H., Eisa T. A. E., Al Dhaqm A., Nasser M., Elhassan T., Elshafie H. & Saif A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences*, *19*(12), 9637.

Alvarado Zabala J., Martillo Alchundia I. & Guzman Seraquive G. (2022). Literature review on Machine Learning techniques in bank fraud detection. *Sapienza: International Journal of Interdisciplinary Studies*, *1*(3), 719–727. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/257

Bol S. & Kros J. (2022). Machine learning for fraud detection in banking: A survey. *Journal of Financial Technology*, *3*(10), 145–167.

Caprian I. & Ţîrlea M. R. (2024). Fraud Risk Management in Banking Activities within Metaverse. *Univers Strategic*, *59*(3), 69–78. https://ibn.idsi.md/sites/default/files/imag_file/69-78_18.pdf

Caprian I. & Ţîrlea M. R. (2024). The Banker of the Future: Characteristics and Trends. *Knowledge-Based Organization*, *2*(30), 101–115. https://doi.org/10.2478/kbo-2024-0057

Caprian I. (2022). The Innovative Activity of the Banks in the Republic of Moldova. *RSES*, 7, 1–10. https://rses.ince.md/items/7be37d18-62c3-485d-83ba-6b43e6376b1d

Caprian I. (2024). Particularităţile utilizării machine learning în scopul detectării fraudei bancare. *Universitatea de Stat din Moldova*. https://economy.studiamsu.md/nr-11-3/

Caprian I. (2022). Modern Approaches to Bank Fraud. *Univers Strategic*, *51*(3), 125–135.

Chauhan S., Singh R. & Sharma P. (2023). AI-driven Fraud Detection: Trends, Challenges, and Implementation in Banking. *International Journal of Financial Technology*, *2*(15), 45–68.

Chen Y. & Wang G. (2021). Big Data Architectures for Real-Time Transaction Monitoring. *International Journal of Data Analytics*, *2*(5), 89–110.

El Harras A. & Salahddine A. (2025). RegTech and AI for Fraud Prevention in Banking: A Systematic Review. *Journal of Financial Regulation and Compliance*, *1*(33), 112–135.

European Banking Authority. (2020). RegTech Report: The Rise of Regulatory Technology in Banking.

FATF (Financial Action Task Force). (2019). Guidance on Digital Identity.

Goodfellow I., Bengio Y. & Courville A. (2016). *Deep Learning*. MIT Press.

Imran M. A. U. (2024). Combating Banking Fraud with IT: Integrating Machine Learning and Data Analytics. *The American Journal of Management and Economics Innovations*, *07*(6), 39–56. https://inlibrary.uz/index.php/tajmei/article/view/36097

Kshetri N. (2018). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy*, *4*(42), 319–335.

Lee J. & Park S. (2023). Explainable AI for Anti Money Laundering: Opportunities and Challenges. *AI & Law Review*, *1*(12), 40–58.

McKinsey & Company. (2021). The Future of Financial Crime: Why Banks Are Investing in AI and Analytics.

Molnar C. (2023). *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*. Leanpub.

OECD. (2022). RegTech for Financial Institutions: Benefits, Risks and Policy Implications.

Wamba S. F. & Akter S. (2019). Big Data Analytics for Fraud Detection: A Review. *Journal of Business Research*, 102, 356–365.

Zanke P. (2023). AI Driven Fraud Detection Systems: A Comparative Study across Banking, Insurance, and Healthcare. *Advances in Deep Learning Techniques*, *2*(3), 1–22.

Стаття надійшла до редакції 08.01.2026 р.

Статтю прийнято до публікації 25.01.2026 р.

Оприлюднено 23.04.2026 р.