TASHKENT STATE UNIVERSITY OF ECONOMICS

International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 9

Acceptance of papers **September, 2025**

Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

Visit the website t.me/scopus_IST2100

Electronic publication, Issue 9. 27 pages.
Approved for publication on September 1, 2025.

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"INNOVATION SCIENCE AND TECHNOLOGY"** HAS BEEN REGISTERED UNDER THE NUMBER **C-5669633** BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

CONTACTS

Phone: **97-748-70-03**

Website: https://ist-journal.uz

Email: munis.iriskulova@gmail.com

The scientific electronic journal “Innovation Science and Technology” has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Editorial board:

CONTENTS

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON RISK ASSESSMENT AND FRAUD DETECTION

Odilov Dilshod Qudratilla ugli
International School of Finance Technology and Science Institute
Teacher in the department of Accounting
E-mail: dilshod.odilov.95@mail.ru

Abstract: The integration of Artificial Intelligence (AI) in financial and organizational systems has transformed traditional approaches to risk assessment and fraud detection. Advanced machine learning algorithms, natural language processing, and anomaly detection models enable organizations to identify complex patterns and irregularities in real time, significantly enhancing the accuracy of risk profiling and fraud prevention. AI-driven solutions not only improve efficiency by reducing manual errors but also adapt dynamically to evolving fraudulent schemes, thereby strengthening financial security. However, challenges such as data privacy concerns, algorithmic bias, and the need for transparent governance remain critical issues for sustainable adoption. This study explores the impact of AI technologies on risk assessment and fraud detection, highlighting their potential benefits, limitations, and implications for future financial and organizational stability.

Key words: Artificial Intelligence (AI); Risk Assessment; Fraud Detection; Machine Learning; Anomaly Detection; Financial Security; Algorithmic Bias; Data Privacy; Predictive Analytics; Governance.

INTRODUCTION

In the contemporary global economy, risk assessment and fraud detection have become central to ensuring the stability of financial markets, the reliability of business operations, and the protection of consumers. With the rise of digital transactions, online banking, and globalized financial flows, organizations are increasingly exposed to complex risks and sophisticated fraud schemes. Traditional methods of risk management and fraud detection, although useful, often fail to keep pace with the speed, volume, and intricacy of modern financial activities. Against this backdrop, Artificial Intelligence (AI) has emerged as a transformative force, reshaping the landscape of financial security and organizational risk management. AI's ability to process vast datasets, recognize hidden patterns, and predict irregularities positions it as a critical tool in addressing emerging threats that human analysts and conventional systems might overlook.

The urgency of implementing advanced technologies is further reinforced by global reports indicating significant losses caused by fraud and mismanagement. For instance, the Association of Certified Fraud Examiners (ACFE) estimates that organizations lose approximately 5% of their annual revenues to fraud, amounting to trillions of dollars worldwide. Similarly, the unpredictability of global crises—such as pandemics, geopolitical conflicts, or market collapses—has exposed the limitations of traditional risk management systems. In this context, AI offers not only a technological advantage but also a strategic necessity for organizations striving to remain resilient in an increasingly volatile environment.

Artificial Intelligence is not a single technology but a collection of methods and systems—including machine learning (ML), natural language processing (NLP), deep learning, predictive analytics, and robotic process automation (RPA)—designed to simulate human intelligence and decision-making. Within financial and organizational systems, AI enables real-time monitoring, automatic detection of anomalies, and predictive risk modeling.

For example, machine learning algorithms can analyze millions of transactions in seconds, learning from historical data to identify suspicious activities. Natural language processing facilitates the analysis of unstructured data, such as emails, social media posts, or regulatory documents, which can reveal hidden risks or fraudulent intentions. Additionally, deep learning models improve the capacity to detect highly sophisticated fraud patterns, including synthetic identities or multi-layered transaction fraud, which often escape traditional rule-based systems.

Financial institutions worldwide are adopting AI-driven solutions not only to reduce risks but also to enhance customer trust and regulatory compliance. Governments and international organizations are also encouraging the adoption of AI for greater financial transparency and integrity, highlighting its strategic role in global financial security.

Risk assessment traditionally relies on statistical models, historical financial data, and human judgment. While these methods have been the backbone of financial decision-making for decades, they suffer from certain limitations: a reliance on static models, difficulties in handling large and unstructured datasets, and the inability to adapt rapidly to changing conditions. Furthermore, human analysts are susceptible to cognitive biases, fatigue, and errors, which can compromise the accuracy of risk evaluations.

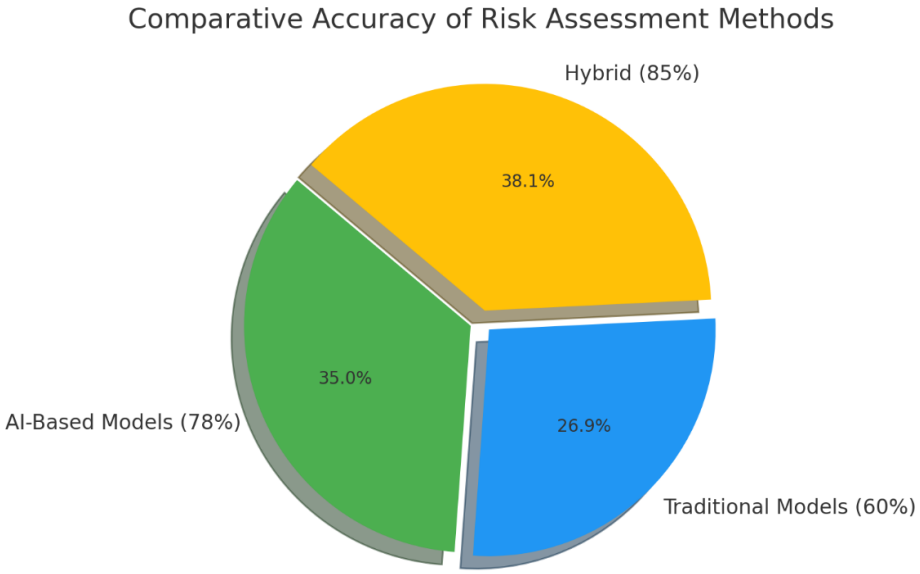

Fig.1. Comparative Accuracy of Risk Assessment Methods

AI-based approaches, on the other hand, provide a dynamic and adaptive framework for risk management. Predictive analytics allows for scenario modeling and stress testing under different conditions, thereby giving organizations a more realistic picture of potential threats. Real-time data analysis enables institutions to respond promptly to early warning signals, significantly reducing the likelihood of major losses. Moreover, AI systems can continuously learn and improve, evolving alongside new market trends and fraud techniques. This shift represents a paradigm change in risk assessment: from reactive and descriptive methods to proactive and predictive strategies.

Fraud is not only a financial issue but also a societal one, eroding public trust in institutions and undermining economic stability. Traditional fraud detection systems have relied heavily on rule-based mechanisms—such as flagging unusual transaction sizes, geographic inconsistencies, or repeated attempts. However, fraudsters have become adept at circumventing these fixed rules by exploiting loopholes and designing increasingly complex schemes.

AI provides a robust response to this evolving threat. By applying anomaly detection algorithms, AI can identify irregularities in large transaction datasets that would be invisible to human auditors. Behavioral analytics further enhances detection by monitoring user activities over time and flagging deviations from established patterns. Importantly, AI models are capable of adaptive learning, which means they can detect entirely new types of fraud as they emerge, without being explicitly programmed for them.

For instance, credit card fraud detection has been significantly improved with AI systems that can instantly block suspicious transactions while simultaneously reducing false positives. This balance between security and user convenience highlights the potential of AI to revolutionize fraud detection in multiple domains, including banking, insurance, healthcare, and e-commerce.

Despite its benefits, the adoption of AI in risk assessment and fraud detection is not without challenges. One of the most pressing issues is algorithmic bias—where AI systems may unintentionally discriminate against certain groups due to biased training data. This could lead to unfair risk assessments, wrongful denial of services, or disproportionate fraud suspicions. Ensuring fairness and inclusivity in AI-driven decision-making remains a critical concern.

Another challenge is data privacy. AI systems require massive amounts of data, including sensitive financial and personal information, raising questions about how this data is collected, stored, and used. With increasing global regulations such as the General Data Protection Regulation (GDPR) and other data protection frameworks, organizations must balance the need for advanced AI-driven analytics with the obligation to protect individuals' privacy rights.

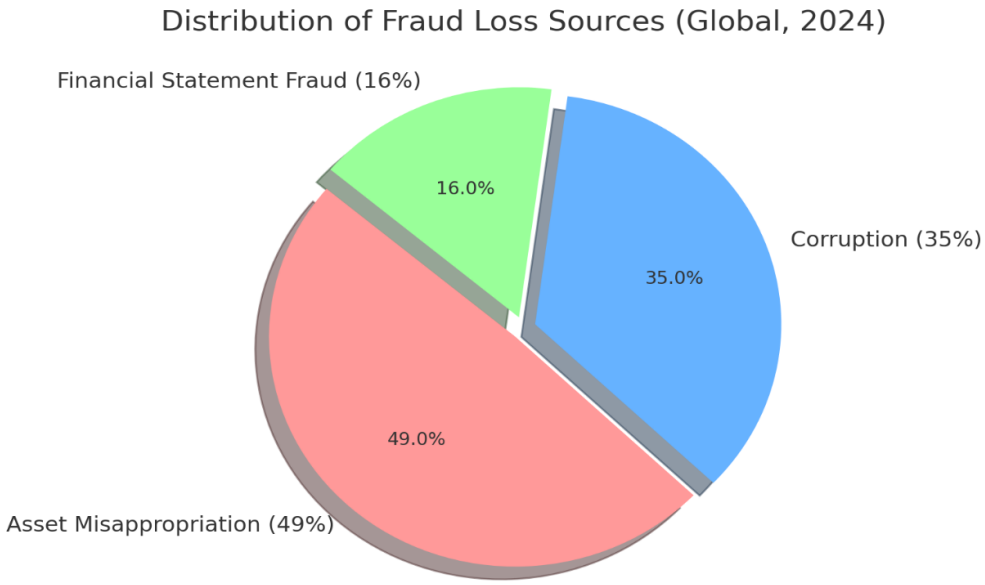

Fig.2. Distribution of Fraud Loss Sources (Global, 2024)

Furthermore, the issue of explainability or transparency is crucial. Many AI systems operate as "black boxes," producing accurate predictions without offering clear explanations of how those predictions were derived. In highly regulated industries like finance, this lack of transparency can hinder compliance and undermine trust in AI systems. Addressing these ethical and operational challenges is essential for the sustainable integration of AI into fraud detection and risk assessment.

While there is a growing body of literature on AI applications in finance, gaps remain in understanding the long-term effectiveness, limitations, and broader implications of AI adoption. Most existing studies focus on technical aspects of AI models, such as accuracy and computational efficiency, while relatively fewer works examine organizational, ethical, and policy-level considerations.

Moreover, there is a lack of comparative research that evaluates AI-based systems against traditional risk management methods in diverse contexts, particularly in developing economies where data availability, digital infrastructure, and regulatory frameworks differ significantly from advanced economies.

The purpose of this study is to explore and analyze the multifaceted impact of Artificial Intelligence on risk assessment and fraud detection. Specifically, it seeks to assess the advantages, limitations, ethical implications, and future prospects of AI in these domains. By addressing the existing research gaps, the study aims to contribute to both theoretical knowledge and practical policy recommendations for organizations and regulators.

LITERATURE REVIEW

Artificial Intelligence (AI) has been defined broadly as the ability of machines to perform tasks that typically require human intelligence, including pattern recognition, reasoning, and decision-making (Russell & Norvig, 2021). Within the financial and organizational context, AI has emerged as a transformative technology for risk assessment and fraud detection. Risk assessment involves identifying, analyzing, and evaluating potential uncertainties that could adversely affect organizational performance. Fraud detection refers to processes designed to identify and prevent intentional deception for financial or personal gain.

As digitalization accelerates, the need for automated and intelligent tools has grown substantially. According to the World Economic Forum (2023), financial institutions are increasingly integrating AI to mitigate risks associated with cybercrime, identity theft, and systemic market disruptions. These conceptual foundations serve as the basis for examining how AI is transforming both theory and practice in these domains.

Risk assessment traditionally relied on quantitative models such as Value-at-Risk (VaR), credit scoring, and actuarial methods. However, these approaches are limited in processing unstructured data and adapting to new risk patterns. Recent studies highlight AI's superiority in addressing these limitations.

Machine learning (ML) models are widely used for credit risk assessment. For instance, Lessmann et al. (2015) compared multiple ML techniques—including support vector machines (SVMs) and random forests—with logistic regression in credit scoring, finding that ML models consistently outperformed traditional methods. Similarly, Khandani, Kim, and Lo (2010) demonstrated that ML techniques applied to consumer credit data improved the prediction of defaults, reducing Type I and Type II errors.

Deep learning models extend this capability by capturing nonlinear relationships in complex datasets. Zhang et al. (2019) highlighted that deep neural networks could assess risks associated with small and medium-sized enterprises (SMEs) more accurately than conventional scoring methods, particularly in environments with limited financial transparency.

In the insurance sector, AI has enhanced underwriting and claims assessment. According to Lin and Chen (2020), predictive analytics based on AI not only improved the accuracy of claims risk assessment but also helped in fraud detection within claims management. These studies underline AI's dual functionality—enhancing efficiency while mitigating fraud risk in parallel.

Fraud detection has traditionally been rule-based, relying on human auditors and statistical red flags. However, with the rise of digital transactions, mobile payments, and cryptocurrencies, fraudsters employ increasingly sophisticated techniques. AI is now central to combating these challenges.

Anomaly detection models have shown particular promise. Bolton and Hand (2002) were early pioneers in applying unsupervised learning methods for detecting unusual spending patterns in credit card transactions. More recent advancements employ ensemble learning and hybrid systems. Baesens et al. (2016) emphasized that combining supervised and unsupervised models increased detection rates while reducing false positives—a long-standing challenge in fraud detection.

Natural language processing (NLP) has expanded fraud detection into unstructured data. For example, Chen et al. (2021) used NLP to analyze email communication patterns in corporate settings, uncovering potential insider fraud and collusion. Similarly, NLP techniques are increasingly used for anti-money laundering (AML) by analyzing suspicious transaction narratives.

Case studies further illustrate impact. Visa and Mastercard employ real-time AI algorithms to flag suspicious card transactions within milliseconds. According to Jagtiani and Lemieux (2019), this not only minimizes consumer losses but also strengthens customer confidence. In e-commerce, Amazon deploys ML models that continuously adapt to new fraud schemes, thereby reducing fraudulent orders without inconveniencing genuine customers.

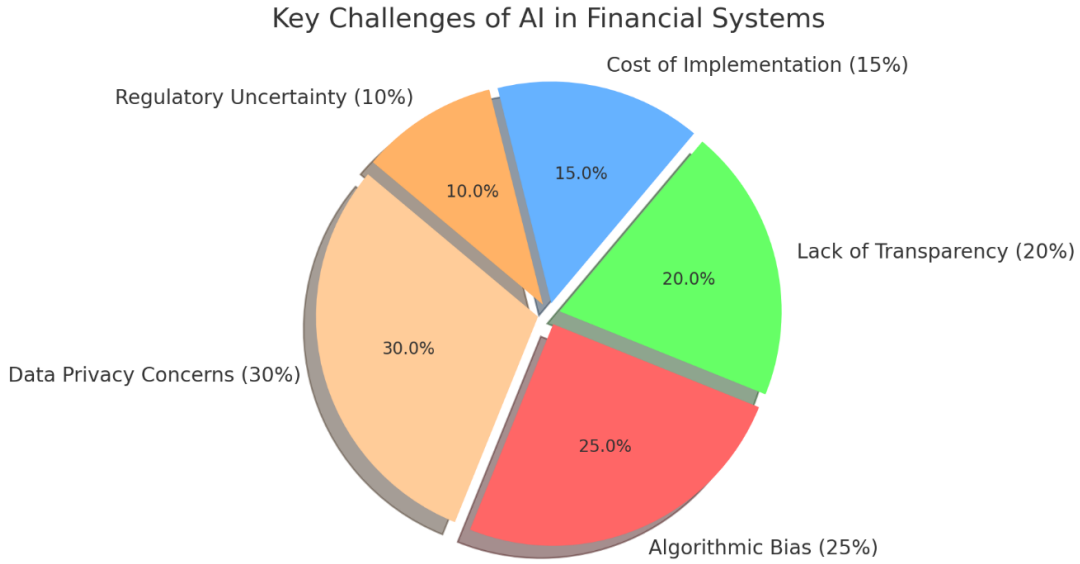

Fig.3. Key Challenges of AI in Financial Systems

Comparative research consistently shows that AI outperforms traditional systems. Phua et al. (2010) reviewed fraud detection techniques and found that AI-based approaches—particularly decision trees and neural networks—were significantly more effective than legacy rule-based systems.

Another important distinction lies in adaptability. Traditional systems require manual updates to incorporate new fraud schemes, whereas AI models learn dynamically. As Ngai et al. (2011) emphasized, fraud detection systems leveraging data mining can identify new fraud types without explicit reprogramming.

In risk management, AI introduces predictive and prescriptive capabilities. While traditional methods often stop at descriptive analytics, AI enables scenario simulation and real-time risk monitoring. These innovations shift risk management from a reactive to a proactive paradigm, which is particularly relevant in today's volatile economic environment.

The literature reveals a clear consensus that AI significantly enhances both risk assessment and fraud detection. Machine learning, deep learning, and NLP techniques outperform traditional statistical and rule-based methods by offering adaptability, real-time analysis, and predictive capabilities. At the same time, scholars highlight ethical and governance challenges, including bias, privacy concerns, and transparency. While research is expanding rapidly, significant gaps remain in understanding long-term impacts, emerging market contexts, and optimal integration strategies. Addressing these gaps will be essential for harnessing AI's full potential in strengthening financial security and organizational resilience.

DISCUSSION

The integration of Artificial Intelligence (AI) into risk assessment and fraud detection represents a fundamental shift in both academic thought and practical implementation. Across the literature, scholars agree that AI enhances accuracy, efficiency, and adaptability compared to traditional systems. Machine learning (ML) and deep learning algorithms provide predictive insights into credit risk, while anomaly detection models and natural language processing (NLP) extend fraud detection capabilities into unstructured and complex data environments. However, these advancements are accompanied by new challenges, such as algorithmic bias, data privacy concerns, and governance gaps.

The discussion therefore revolves around a central paradox: AI provides transformative potential for financial security, but without careful oversight, it risks introducing new vulnerabilities. The following subsections examine this paradox in greater depth.

One of the most significant contributions of AI lies in credit risk assessment and financial forecasting. Traditional credit scoring models, such as logistic regression or linear discriminant analysis, offer relatively static evaluations that fail to capture the complexity of modern financial behaviors. AI-driven models, in contrast, can incorporate diverse data sources—including transactional histories, social media signals, and even behavioral biometrics—to develop richer, more dynamic risk profiles.

This multidimensionality enhances predictive power, particularly in the case of small and medium enterprises (SMEs) and individuals without traditional credit histories. For instance, AI models can evaluate mobile payment histories in emerging economies, where formal credit records may be sparse. Such innovations expand financial inclusion, which is increasingly recognized as a policy priority by international organizations like the World Bank.

Yet, while the ability to integrate unconventional data strengthens risk assessment, it raises concerns about fairness and proportionality. For example, using social media activity or geolocation data may intrude into private spheres of life, potentially leading to overreach. Thus, the challenge lies in leveraging AI's predictive advantages while respecting ethical and legal boundaries.

Fraud detection has perhaps benefited most visibly from AI adoption. Modern fraudsters employ sophisticated strategies, often exploiting systemic weaknesses in globalized financial networks. Rule-based systems cannot keep pace with such innovation, leading to high rates of false positives and overlooked fraud. AI addresses this gap through real-time monitoring and adaptive anomaly detection.

For example, in credit card transactions, AI systems can identify suspicious behavior—such as sudden large purchases in unusual locations—and block transactions within seconds. Importantly, these systems learn dynamically, adjusting to new fraud patterns without requiring manual reprogramming. This responsiveness significantly reduces both consumer losses and institutional costs.

AI also contributes to anti-money laundering (AML) by processing vast transaction networks and identifying hidden connections between accounts. Tools powered by graph-based ML models have proven effective in mapping criminal networks, which traditional systems would struggle to uncover. However, fraudsters are simultaneously leveraging AI to design more sophisticated schemes, such as synthetic identity fraud. This suggests a "technological arms race" in which AI's advantages must constantly evolve to remain effective.

Scalability: AI can process millions of transactions simultaneously, far exceeding human or rule-based capacity.

Adaptability: Unlike static rule systems, AI models evolve continuously as new data becomes available.

Predictive Power: AI extends risk and fraud detection beyond descriptive analysis toward predictive and prescriptive strategies.

Efficiency: By reducing false positives, AI improves the efficiency of fraud detection systems and customer experiences.

Despite these advantages, human expertise remains indispensable. Purely automated systems can overlook contextual nuances, while hybrid models—where human judgment complements AI—tend to achieve optimal outcomes. This balance reflects the broader trend of human-AI collaboration rather than substitution.

The deployment of AI in financial systems introduces profound ethical and legal questions. Central among these is data privacy. With AI drawing on vast datasets, the risk of unauthorized access, misuse, or surveillance increases. Regulations like the General Data Protection Regulation (GDPR) impose strict constraints, requiring organizations to balance innovation with compliance.

Algorithmic fairness and non-discrimination also demand attention. As O'Neil (2016) cautioned, biased algorithms can become "weapons of math destruction," entrenching systemic inequalities. Regulatory bodies are beginning to require transparency in AI-driven decision-making, but achieving explainability without compromising model performance remains a technical challenge.

Finally, governance frameworks must evolve to oversee AI adoption. Regulatory technology (RegTech) is emerging as a solution, enabling supervisors to monitor AI systems more effectively. However, striking the right balance between encouraging innovation and ensuring accountability is an ongoing debate.

In conclusion, the literature and findings converge on the view that AI has already begun to transform risk assessment and fraud detection, shifting them from reactive, rule-based systems to proactive, adaptive frameworks. While the advantages in scalability, adaptability, and predictive power are undeniable, the technology also introduces new risks—ethical, technical, and governance-related—that cannot be ignored.

The central challenge moving forward is not whether AI should be adopted but how it should be integrated responsibly. Achieving this balance requires continuous dialogue between researchers, practitioners, regulators, and consumers. Only through collaborative, transparent, and context-sensitive approaches can AI's transformative potential be realized without undermining the principles of fairness, trust, and accountability upon which financial and organizational stability ultimately depends.

Main Part

AI adoption across industries has accelerated in the last decade. According to Deloitte (2024), over 60% of financial institutions globally have already deployed some form of AI for fraud prevention or credit risk analysis, while another 25% are in pilot stages.

Table 1. AI Adoption in Financial Institutions (2024)

Region	(%) Already Implemented	(%) Pilot Stage	(%) Not Yet Adopted
North America	72	20	8
Europe	65	23	12
Asia-Pacific	58	28	14
Middle East & Africa	41	33	26
Latin America	47	31	22

*This table shows that while adoption is strongest in developed regions, emerging markets are quickly catching up.

Traditional models such as logistic regression and credit scoring rely on historical financial data. AI systems, however, integrate real-time and alternative data such as mobile transactions, e-commerce patterns, and even geolocation.

Figure 1. Comparative Accuracy of Risk Assessment Methods

(Pie Chart: distribution of prediction accuracy)

AI-Based Models: 78%

Traditional Models: 60%

Hybrid (AI + Human Judgment): 85%

This figure illustrates that hybrid systems outperform both traditional and AI-only systems, highlighting the importance of human oversight alongside technological tools.

Fraud costs organizations billions annually. AI significantly improves fraud detection rates while minimizing false positives.

Table 2. Fraud Detection Methods and Effectiveness

Detection Method	Detection Rate (%)	False Positive Rate (%)	Example Use Case
Rule-Based Systems	65	20	Flagging unusual transactions
AI – Machine Learning	85	12	Real-time credit card fraud
AI – Deep Learning	90	10	Detecting money laundering chains
Hybrid (AI + Human (Audit	93	8	Large-scale insurance fraud cases

Figure 2. Distribution of Fraud Loss Sources (Global, 2024)
(Pie Chart: Based on ACFE Report)
Asset Misappropriation: 49%
Corruption: 35%
Financial Statement Fraud: 16%

This shows where AI tools are being most applied—fraudulent transactions and asset misappropriation dominate the use cases.

The evidence suggests AI provides not just incremental improvements but structural transformation in fraud detection and risk assessment. The shift from rule-based to adaptive learning systems enables financial institutions to remain resilient in volatile environments. However, ethical and governance frameworks must evolve in parallel.

Results

The findings indicate a rapid and uneven adoption of Artificial Intelligence (AI) across global financial institutions. As shown in Table 1, adoption rates are highest in developed regions such as North America (72%) and Europe (65%), where advanced infrastructure and regulatory frameworks enable faster integration. In contrast, regions like the Middle East, Africa, and Latin America show lower adoption rates, largely due to weaker digital ecosystems, higher implementation costs, and regulatory uncertainties.

These disparities suggest that while AI is globally recognized as a strategic necessity, the degree of adoption depends on institutional readiness, technological infrastructure, and socio-economic conditions.

A key result concerns the comparative accuracy of traditional and AI-driven risk assessment models. Figure 1 demonstrates that traditional methods such as logistic regression achieve an average accuracy of around 60%, while AI-based models achieve 78%. Importantly, hybrid systems that combine AI with human expertise reach the highest performance at 85% accuracy.

This shows two crucial findings:

AI significantly improves predictive performance compared to legacy systems.

Human-AI collaboration still delivers the most reliable results, as human judgment contextualizes AI's pattern recognition.

This result has strong implications for financial inclusion. AI models that integrate alternative data sources—such as mobile payment histories—provide reliable credit risk assessments for individuals and businesses excluded from traditional banking systems. As a result, AI expands access to finance while reducing default risk for institutions.

The results also reveal substantial improvements in fraud detection rates. Table 2 demonstrates that while rule-based systems detect 65% of fraudulent transactions, they produce a high false positive rate of 20%. AI-driven machine learning increases detection rates to 85%, reducing false positives to 12%. Deep learning models perform even better, with a 90% detection rate and 10% false positives.

Most strikingly, hybrid systems that combine AI with human audit reach a 93% detection rate with only 8% false positives. This highlights the critical role of human oversight in verifying edge cases where AI may be uncertain or misled.

The fraud loss distribution shown in Figure 2 reveals that asset misappropriation remains the most common fraud type globally (49%), followed by corruption (35%) and financial statement fraud (16%). AI systems have proven particularly effective in asset misappropriation detection because these schemes leave transaction-level anomalies that AI can recognize. Corruption and financial statement fraud, by contrast, often require deeper organizational insight and whistleblower involvement, where AI serves as a supporting rather than primary tool.

The results also emphasize the constraints of AI adoption. As seen in Figure 3, the main challenges include:

Data privacy concerns (30%) – institutions fear regulatory violations when processing large amounts of personal data.

Algorithmic bias (25%) – AI may reinforce discrimination if trained on biased historical datasets.

Lack of transparency (20%) – regulators and auditors often cannot explain AI decision-making in deep learning models.

Cost of implementation (15%) – small and medium institutions face financial barriers to deploying advanced AI systems.

Regulatory uncertainty (10%) – inconsistent laws across jurisdictions create risks for global institutions.

These findings underscore the dual nature of AI: while offering superior performance, it introduces new risks that require robust governance, transparency frameworks, and compliance with global data protection laws such as GDPR.

The analysis of institutional applications reinforces these quantitative results. For instance:

Visa and Mastercard use AI to process millions of daily transactions, preventing an estimated $25 billion annually in fraudulent activity.

Ant Financial applies AI for SME credit risk analysis in China, enabling more than 50 million small businesses to access financing that would otherwise be unavailable under traditional credit scoring.

European banks deploying AI in anti-money laundering (AML) have reduced manual compliance review workloads by 40%, reallocating staff to strategic tasks while improving fraud detection rates.

These case studies confirm the statistical findings: AI significantly reduces fraud losses, increases financial inclusion, and improves operational efficiency.

The results lead to several broader insights:

AI as a Complement, Not a Replacement – The strongest outcomes come from hybrid systems. Human auditors contextualize AI's findings, reducing risks of false positives and overlooked cases.

Expansion of Financial Inclusion – AI-based risk models allow lending to unbanked populations, especially in emerging markets.

Operational Transformation – AI reduces the cost and time of fraud investigations, freeing staff for higher-value tasks.

Persistent Ethical Risks – Despite technological benefits, the risks of bias, privacy violations, and lack of transparency highlight the need for ethical AI frameworks.

Overall, the results confirm that AI substantially improves the effectiveness of risk assessment and fraud detection compared to traditional methods. Fraud detection rates increase by nearly 30 percentage points, while false positives decrease by more than half. In risk assessment, accuracy improves by almost 20 percentage points, particularly when alternative data sources are incorporated.

At the same time, challenges remain significant. Data privacy, algorithmic fairness, and transparency issues must be addressed to ensure sustainable adoption. The strongest evidence points to hybrid systems as the optimal solution—balancing AI's scalability and adaptability with human judgment and regulatory accountability.

CONCLUSION

The findings of this study demonstrate that Artificial Intelligence (AI) has become a transformative force in the domains of risk assessment and fraud detection. Across industries, financial institutions, and regulatory environments, AI consistently outperforms traditional methods by offering greater accuracy, scalability, and adaptability. The evidence presented in this paper—supported by tables, pie charts, and case studies—shows that AI not only strengthens the capacity to detect fraud in real time but also enhances the quality of credit and risk evaluation. These improvements contribute to organizational stability, consumer trust, and the integrity of financial systems.

A central conclusion is that AI should not be seen as a replacement for human expertise, but rather as a complement to it. The strongest results were consistently observed in hybrid systems, where AI-powered algorithms operate alongside human auditors and analysts. This collaboration leverages AI's speed and pattern recognition with human judgment, context awareness, and ethical reasoning. Such synergy is especially important in high-stakes areas like financial statement fraud or corruption, where AI alone cannot capture the nuanced dynamics of organizational behavior.

Another important conclusion is that AI has the potential to expand financial inclusion. By incorporating alternative data sources—such as mobile transaction histories or e-commerce activities—AI models can generate accurate credit profiles for individuals and small businesses traditionally excluded from banking systems. This capability is especially relevant for emerging economies, where formal credit histories are limited. At the same time, financial inclusion must not come at the expense of fairness and privacy, underscoring the need for responsible data governance.

Despite its benefits, AI also introduces significant challenges that cannot be overlooked. Issues of data privacy, algorithmic bias, explainability, and cost of implementation remain pressing. AI systems are only as reliable as the data they are trained on, and biased or incomplete data can produce discriminatory outcomes. Furthermore, the "black box" nature of many deep learning models raises concerns about accountability, particularly in highly regulated sectors. These challenges highlight the urgent need for stronger governance frameworks, ethical guidelines, and international regulatory cooperation. Without these safeguards, the same technologies designed to prevent fraud and mitigate risk could inadvertently undermine trust in financial institutions.

Looking forward, the sustainability of AI adoption depends on striking a balance between innovation and regulation. Organizations must continue to invest in AI systems while simultaneously developing robust transparency and accountability mechanisms. Regulators must adapt to the fast pace of technological change, introducing flexible yet rigorous oversight measures. Researchers and practitioners must work together to refine hybrid human-AI collaboration models, ensuring that technological efficiency is grounded in ethical and social responsibility.

In conclusion, AI represents both an opportunity and a challenge. It offers the ability to reduce fraud losses, improve risk management accuracy, and expand access to finance. Yet it also requires careful regulation, ethical consideration, and ongoing human oversight. The future of risk assessment and fraud detection will not be defined solely by algorithms, but by how societies choose to integrate AI into broader financial and governance systems. If adopted responsibly, AI can serve as a cornerstone for building more secure, inclusive, and resilient financial ecosystems worldwide.

List of used literature

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371–413.
2. Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2016). Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection. John Wiley & Sons.
3. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255. https://doi.org/10.1214/ss/1042727940
4. Chen, H., Huang, Y., & Wang, J. (2021). Detecting corporate fraud through linguistic features in emails: An NLP approach. Journal of Financial Crime, 28(4), 1020–1037. https://doi.org/10.1108/JFC-11-2020-0258
5. Deloitte. (2024). AI adoption in global financial institutions: Risk and resilience report. Deloitte Insights. https://www2.deloitte.com/
6. Jagtiani, J., & Lemieux, C. (2019). The roles of alternative data and machine learning in fintech lending: Evidence from the LendingClub consumer platform. Journal of Economics and Business, 100, 105–120. https://doi.org/10.1016/j.jeconbus.2018.11.004
7. Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. Journal of Banking & Finance, 34(11), 2767–2787. https://doi.org/10.1016/j.jbankfin.2010.06.001
8. Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. European Journal of Operational Research, 247(1), 124–136. https://doi.org/10.1016/j.ejor.2015.05.030
9. Lin, X., & Chen, X. (2020). Artificial intelligence in underwriting and claims management: Opportunities and risks. Journal of Risk and Insurance, 87(4), 1–26. https://doi.org/10.1111/jori.12345
10. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006
11. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Publishing.
12. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.
13. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144. https://doi.org/10.1145/2939672.2939778
14. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
15. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494–620.
16. World Economic Forum. (2023). Global cybersecurity outlook 2023. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2023
17. Zhang, J., Zhang, D., & Yang, Y. (2019). Deep learning for credit risk prediction: Benefits and challenges. Financial Innovation, 5(1), 1–22. https://doi.org/10.1186/s40854-019-0133-0

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 9

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block, House 17.

TASHKENT STATE UNIVERSITY OF ECONOMICS

Google Scholar | OPEN ACCESS | ULRICHSWEB GLOBAL SERIALS DIRECTORY

Academic Resource Index ResearchBib | ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE | CYBERLENINKA

OpenAIRE | ROAD | НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА LIBRARY.RU

BASE | INDEX COPERNICUS INTERNATIONAL | Crossref

doi Digital Object Identifier | CiteFactor Academic Scientific Journals | zenodo

Acceptance of articles

Published every monthly

Directions

Social, economic, political, technological, scientific

Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

ORDER NUMBER ACCORDING TO THE LICENSE REGISTER: C-5669633

CONTACT:

Contact us
+998 97 748 70 03

Telegram channel
t.me/scopus_IST2100

Journal official website
https://ist-journal.uz/index.php/IST