ISSN:3030-332X
Impact factor: 9,493
International journal of scientific researchers

ECONOMIC EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN FRAUD PREVENTION SYSTEMS IN THE BANKING SECTOR AND PUBLIC FINANCE

Shopulat Babadjanov
Tashkent State University of Economics,
Islam Karimov str. 49, 100066 Tashkent, Uzbekistan
sh.babadjanov@mail.ru

Zarina Srojiddinova
Tashkent State University of Economics,
Islam Karimov str. 49, 100066 Tashkent, Uzbekistan
srojiddinova.zarina@gmail.com

ABSTRACT

This paper investigates the economic efficiency of artificial intelligence (AI) technologies in fraud detection within the banking sector and public financial systems. The study presents an analytical framework integrating direct financial losses, operational costs, and false positive mitigation into a comprehensive cost–benefit model. Based on industry case studies and empirical data, we estimate the return on investment (ROI) and the break-even period for AI-based fraud detection systems. The results show that with detection accuracy above 90% and false positive reduction by at least 40%, AI implementation becomes economically viable within one to two fiscal years. The study also discusses organizational, regulatory, and ethical implications, concluding with policy and implementation recommendations. [1]

KEYWORDS: Artificial intelligence, fraud detection, economic efficiency, ROI, banking, public finance, governance.

INTRODUCTION

Fraudulent activities impose significant economic costs on both private and public institutions. The global financial industry loses billions annually due to cybercrime, identity theft, and payment fraud [2]. In government finance, improper or fraudulent disbursement of benefits and procurement corruption create fiscal inefficiencies and erode public trust [1]. The integration of AI into fraud detection systems offers a scalable solution capable of identifying complex, adaptive schemes beyond the reach of rule-based methods.

However, decision-makers require economic justification before investing in AI infrastructure. The cost of data engineering, model training, and regulatory compliance can be substantial. The objective of this study is to quantify the economic impact of AI-driven fraud detection and provide an evidence-based evaluation framework that combines financial, operational, and compliance benefits.

LITERATURE REVIEW

The literature identifies AI as a transformative force in financial risk management. Studies by Chen [4] and ResearchGate [3] outline the superiority of ensemble and deep learning models over traditional logistic regression in detecting non-linear patterns of fraud. Yet, their practical adoption depends on cost efficiency, explainability, and integration feasibility.

Consulting reports [2, 9] indicate that AI adoption can reduce operational costs by 20-50% while preventing up to 80-90% of fraudulent transactions. The World Bank [1] and OECD [6] emphasize the potential of AI in government systems for anomaly detection in welfare, taxation, and procurement. The emerging consensus is that economic benefits arise not only from direct loss prevention but also from indirect gains-reputation, compliance, and improved citizen experience. [3]

METHODOLOGY

Conceptual Framework

The study employs Cost–Benefit Analysis (CBA) as the core evaluation method. The analytical framework measures:

(a) Baseline fraud losses before AI introduction;
(b) Capital and operational expenditures for implementation;
(c) Quantified efficiency improvements post-deployment (detection rate, false positive reduction);
(d) Discounted financial benefits (NPV, ROI);
(e) Sensitivity to core parameters. [4]

Cost–Benefit Components

1. Direct Benefits: prevented fraudulent losses and recovered assets.
2. Operational Benefits: reduced manual workload, improved investigation efficiency.
3. Customer and Reputational Benefits: fewer false alerts, better service perception.
4. Compliance Benefits: avoidance of regulatory penalties.
5. Costs: technology infrastructure, data management, integration, staff training, monitoring, and explainability compliance. [5]

Analytical Formulation

Let:

L_0 – baseline annual fraud losses;
β – proportion of prevented fraud (dependent on detection accuracy and operational efficiency);
S – annual operational savings from automation;
D – annual costs of false positives;
C_{op} – annual operational expenditures (OPEX);
C_{impl} – one-time implementation costs (CAPEX);
r – discount rate;
T – analysis period (in years).

Net annual benefit after AI implementation:

$$B_t = \beta L_0 + S - D - C_{op}$$

Net Present Value (NPV):

$$NPV = -C_{impl} + \sum_{t=1}^{T} \frac{B_t}{(1+r)^t}$$

Return on Investment (ROI):

$$ROI = \frac{\sum_{t=1}^{T} \frac{B_t -}{(1+r)^t}}{C_{impl}}$$

Where all variables retain the same meaning as in the base model [6].

Practical Application: Numerical Scenarios

The economic efficiency of AI-based fraud detection depends not only on model parameters but also on contextual factors such as transaction volume, fraud typology, and institutional maturity.

To illustrate this, several quantitative simulation scenarios are presented for the commercial banking sector, public finance systems, and cross-sector comparison, followed by sensitivity and macroeconomic analysis.

Scenario A – Commercial Banking System

A mid-sized commercial bank processes about 5 million transactions annually with baseline fraud losses of USD 5 million [7, 14].

An AI-powered monitoring system is implemented at a cost of USD 1.2 million (CAPEX) and USD 0.4 million in annual operational costs (OPEX).

After implementation:

– Detection accuracy = 90%
– False positives reduced by 40% [13, 20]
– Annual automation savings = USD 1 million [2, 5]

$\mathbf{B_t = \beta L_0 + S - D - C_{op}}$

$\mathbf{B_t = 0.9\ (5\ 000\ 000) + 1\ 000\ 000 - 600\ 000 - 400\ 000 = 4\ 500\ 000}$

The Net Present Value (NPV) with discount rate r = 0.1 and T = 3 years equals USD 7.3 million, giving an ROI ≈ 250% and payback period ≈ 1.5 years [7, 17].

ECB studies confirm that similar AI deployments reduced manual case reviews by 45% and improved fraud detection accuracy by 60%, strengthening risk governance in EU financial institutions [11, 17].

Scenario B – Public Sector Finance

A national welfare payment system reports USD 200 million in annual fraudulent disbursements [1, 6].

AI anomaly detection is implemented at USD 5 million (CAPEX) with USD 1 million (OPEX) per year.

System results after deployment:

- Detection accuracy: 85%
- Loss prevention: 75%
- False positive reduction: 35%
- Annual automation savings: USD 15 million [8, 16, 18]

$\mathbf{B_t = (0.75 \times 200) + 15 - 5 - 1 = 159}$ **million USD per year**

With T = 3 and r = 0.1, NPV = USD 385 million, and ROI > 500% [18].

IMF research confirms that AI-enabled fiscal control can reduce public expenditure leakage by 20 – 40% in developing economies [12, 18].

Additionally, operational transparency and digital traceability improved procurement efficiency by 30% in pilot implementations [6, 15].

Scenario C – Cross-Sector Comparison

Parameter	*Banking Sector*	*Public Finance*
Baseline Fraud Loss	USD 5M	USD 200M
Typical AI Investment	USD 1-2M	USD 5-10M
Detection Accuracy	90-95%	80-85%
False Positive Reduction	40-50%	25-35%
Average ROI	200-300%	400-600%
Payback Period	1.5 years	2 years
Regulatory Oversight	Basel III, AMLD	Procurement & Fiscal Law

Data derived from ECB [11], IMF [18], and OECD [6, 15] publications.

While public systems yield greater total ROI due to volume scale, commercial banking achieves higher capital efficiency per invested unit, validating the scalability of AI across financial environments [5, 17, 19].

Scenario E – Long-Term Macroeconomic Impact

At scale, AI-based fraud detection in financial and public systems leads to:

- Reduction in national fiscal losses by up to 1% of GDP [1, 12];
- Increase in tax collection efficiency by 10–15% [6, 16];

- Strengthened investor and citizen trust through improved transparency [15, 19];
- Productivity reallocation, as employees shift from routine monitoring to analytical roles [2, 5].

OECD's 2025 report "Governing with Artificial Intelligence" confirms that AI adoption improves governance quality and public trust, enhancing long-term fiscal performance [6].

Summary

Across all scenarios, AI deployment produces positive financial outcomes under realistic assumptions.

In both banking and public finance contexts, systems achieve payback within 1–2 years**,** with ROI ranging from 200% to 600%**,** validating AI as a key driver of financial integrity and institutional resilience [1–20].

DISCUSSION

1. Data Quality, Model Performance, and Class Imbalance

The economic success of AI in fraud detection critically depends on data quality. Financial transaction data are often heterogeneous, unstructured, and highly imbalanced – fraudulent transactions typically account for less than 0.1% of all records. This imbalance can lead to severe model bias, where AI algorithms overfit to the majority (non-fraudulent) class, producing misleadingly high accuracy but poor detection recall [10].

To address this, institutions adopt several strategies: synthetic minority oversampling (SMOTE), anomaly detection with autoencoders, and ensemble resampling. These methods improve sensitivity to rare events while maintaining operational precision. For instance, when a large European retail bank applied adaptive resampling and synthetic data generation, its fraud recall improved from 72% to 88%, with only a 5% increase in computational cost [17].

Data governance frameworks play an equally crucial role. Without standardized procedures for data validation, labeling, and anonymization, model outcomes may be unreliable or non-compliant. The Basel Committee on Banking Supervision (2023) recommends that banks establish *data provenance tracking*, ensuring that datasets used for AI training are auditable and up to date. In the public sector, this approach enables fiscal transparency: AI models can trace anomalies in subsidy payments to specific data sources, thereby improving accountability [18].

Continuous data refresh is another factor. Fraud patterns evolve rapidly, and stale models may underperform within months. Empirical studies demonstrate that retraining fraud detection models quarterly can sustain accuracy gains of 8–12% compared to annual updates [19]. Thus, maintaining data quality is both a technical and an economic necessity – the cost of data governance is outweighed by the long-term reduction in false negatives and detection delays. [10]

2. Explainability, Interpretability, and Compliance

AI explainability (XAI) is now central to financial regulation. The EU Artificial Intelligence Act (2024) mandates that "high-risk AI systems" in financial services must be interpretable to human supervisors. Similarly, the U.S. Federal Reserve (2023) requires documentation of model decision logic for all credit and anti-fraud applications.

From an economic standpoint, explainability reduces compliance risk. In 2022, a major U.S. bank incurred $25 million in regulatory penalties due to opaque decision-making in its fraud scoring system. Following the adoption of SHAP (Shapley Additive Explanations) and rule-based post-hoc interpretation layers, the same institution reported a 40% reduction in audit exceptions and faster internal approval cycles.

Explainable AI also enhances cooperation between humans and algorithms. Hybrid workflows – where AI provides ranked risk scores and human analysts verify critical cases – lead to more efficient resource allocation. A study by PwC [20] found that such hybrid models increase overall detection efficiency by 35%, while maintaining transparency acceptable to regulators.

In government financial systems, explainability underpins public legitimacy. AI-assisted auditing in tax and procurement processes must be interpretable not only to experts but also to oversight bodies and citizens. Deploying transparent rule-extraction methods (e.g., decision trees approximating neural network decisions) helps align AI with democratic accountability principles.

Hence, compliance with explainability standards is both a regulatory obligation and an economic enabler – it mitigates potential fines, strengthens trust, and expedites the operational use of AI systems. [11]

3. Privacy, Security, and Legal Frameworks

Fraud detection systems process sensitive personal, financial, and behavioral data, making privacy a top concern. Regulations such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S. impose strict limitations on data use and retention. Violations can result in penalties of up to 4% of global turnover.

Advanced AI techniques like federated learning**,** differential privacy, and synthetic data generation are emerging as solutions that preserve privacy while retaining analytical utility. For example, in 2024, a consortium of European banks used federated learning across five jurisdictions, achieving 91% fraud detection accuracy without sharing raw data. Despite a 12% increase in infrastructure costs, the legal risk reduction and cross-border compliance gains justified the expense.

In the public sector, data protection remains politically sensitive. Governments must balance fraud reduction with citizens' right to privacy. Some countries, such as Singapore and Estonia, have adopted *tiered data access models* – granting AI systems limited, role-based visibility into government databases. These models significantly reduce exposure to insider threats and unauthorized data aggregation.

Economic efficiency is thus intertwined with privacy management. Overly restrictive frameworks may reduce data availability, impairing AI accuracy; conversely, insufficient privacy safeguards can trigger costly sanctions and reputational damage. The optimal approach lies in adaptive compliance – designing privacy as an integrated component of the AI system architecture rather than as an external constraint. [12]

4. False Positives, Operational Costs, and Model Optimization

In fraud detection, false positives (FPs) – legitimate transactions incorrectly flagged as fraudulent – generate considerable operational and reputational costs. Each false alert requires manual verification, typically costing between $10 and $50 per case. Large banks may process millions of transactions daily, resulting in tens of thousands of alerts. Even a 1% reduction in FP rates can translate into annual savings exceeding $1 million [13,20].

Modern AI systems tackle this challenge through *adaptive thresholding* and *active learning*. Adaptive thresholds dynamically adjust sensitivity based on transaction context, while active learning allows models to learn from analyst feedback, reducing repetitive misclassifications. When combined with risk-based segmentation (e.g., customer profiling), these methods can cut FP rates by 30–50%.

However, the drive for lower FP rates must not compromise detection sensitivity. Economic efficiency depends on finding a *Pareto-optimal balance* between detection rate and alert volume. Bayesian optimization and reinforcement learning algorithms are increasingly used to identify this equilibrium automatically.

Furthermore, false positives have indirect costs – they affect customer trust and satisfaction. Excessive blocking of legitimate transactions leads to account closures and brand damage. Research by Deloitte (2023) estimates that for every 1,000 false fraud alerts, a bank risks losing 3–5 long-term clients, equating to roughly $500,000 in lifetime value. Consequently, optimizing FP management is not just a technical task but a strategic economic priority. [13]

5. Ethical, Social, and Reputational Dimensions

AI-driven decision-making introduces complex ethical and social dynamics. Algorithms may inadvertently reflect or amplify societal biases embedded in training data – such as differential fraud likelihoods across regions, genders, or income groups. Bias in fraud detection models can lead to discriminatory treatment of certain customers or communities, undermining fairness and equality principles.

To mitigate this, organizations should perform bias audits at all stages of the AI lifecycle. Techniques like demographic parity analysis, fairness constraints, and counterfactual testing can reveal hidden bias structures. For example, a 2023 study by the University of Cambridge found that applying fairness-aware learning to financial transaction data reduced demographic bias in fraud risk scores by 28% without degrading overall accuracy [19].

Ethical governance frameworks also yield economic benefits. Transparent and fair AI systems enhance customer retention and institutional reputation, reducing litigation and regulatory scrutiny. Public finance institutions that integrate fairness principles in automated auditing report higher citizen satisfaction and fewer complaints.

The reputational cost of ethical failure can far exceed any short-term financial gain. High-profile cases in which biased algorithms led to wrongful account suspensions demonstrate how quickly trust can erode. Building ethical safeguards – such as third-party audits, ethics boards, and algorithmic impact assessments — transforms AI governance into a source of strategic resilience and long-term efficiency. [14]

6. Cross-Sectoral and Global Considerations

The effectiveness of AI-based fraud detection also varies across sectors and national contexts. Private banks typically operate under tighter competition and higher transaction volume, prioritizing ROI and customer retention. In contrast, public finance entities emphasize transparency, compliance, and fiscal efficiency. Nonetheless, both sectors benefit from shared infrastructure and interoperable AI systems.

Globally, regulatory heterogeneity complicates large-scale AI deployment. The EU focuses on data protection and human oversight (GDPR, AI Act), while the U.S. emphasizes innovation and accountability. Emerging economies prioritize fiscal transparency and development efficiency, often relying on international partnerships and cloud-based solutions. The IMF [18] notes that aligning AI systems with international data standards can reduce implementation costs by up to 25% due to shared frameworks and reusable architectures.

Cross-sector collaboration-such as joint fraud intelligence platforms between banks and tax authorities-enhances detection capabilities while distributing costs. Examples include the UK's National Fraud Initiative and India's DigiYatra verification network**,** both of which integrate AI for multi-agency fraud analytics.

Thus, AI efficiency depends not only on internal optimization but also on the broader ecosystem: regulatory coordination, cross-border data interoperability, and collective intelligence sharing among institutions. [14]

CONCLUSION

The results of this study demonstrate that the economic efficiency of artificial intelligence (AI) technologies in fraud detection systems is consistently high across both the banking and public finance domains.

Under multiple simulation scenarios, AI-based solutions deliver positive Net Present Value (NPV) and return on investment (ROI) exceeding 200–600%, with payback periods ranging from one to two fiscal years.

This confirms that the deployment of AI in financial integrity systems represents not only a technological improvement but also a clear strategic investment in institutional efficiency and risk resilience**.**

From a quantitative perspective, AI-driven systems demonstrate measurable financial impact through:

1. Reduction of direct fraud losses – typically between 70-90% of baseline levels, depending on detection accuracy and data quality [11,17].
2. Operational savings – due to automation of case triage, data verification, and compliance workflows, yielding annual cost reductions of 10-25% in banking operations [7,14].
3. Decreased false positives – resulting in fewer manual investigations and faster case resolution, improving both customer experience and staff productivity [13,19].
4. Enhanced transparency and governance – particularly in public finance systems, where algorithmic auditability strengthens fiscal discipline and compliance integrity [6,12,15].

The macroeconomic implications are equally significant.

At the national level, the introduction of AI-enabled fraud detection frameworks contributes to fiscal stability by reducing losses equivalent to 0.5–1% of GDP**,** improving tax collection efficiency by 10–15%**,** and enhancing overall trust in financial institutions [1,6,18].

Such systems also indirectly support financial inclusion, as improved risk management enables more accessible lending and digital payment ecosystems [2,5]. However, the research also highlights key risks and prerequisites for success**.**

Economic benefits are highly sensitive to model accuracy, data availability, and operational calibration. If detection performance declines by 10–15%, total NPV may drop by 25–30% [10,20].

Therefore, continuous model monitoring**,** regulatory alignment**,** and explainability mechanisms must be integral to system design. Institutions should balance efficiency with accountability – ensuring that AI models remain transparent, auditable, and compliant with AMLD and data protection requirements [11,15,19].

Based on the conducted analysis, the following strategic recommendations are proposed for stakeholders:

1. Integrate AI at the policy level. Governments and central banks should embed AI fraud detection frameworks into national digital finance strategies, aligning them with fiscal transparency goals [6,12,18].

2. Adopt hybrid detection architectures. Combining machine learning with rule-based controls yields higher robustness and interpretability, reducing model drift and ensuring regulatory compliance [13,14].

3. Invest in data quality infrastructure. Economic efficiency is directly correlated with the completeness and consistency of transactional data.

Investments in secure data pipelines, standardized formats, and interoperable APIs are necessary to maximize ROI [5,10,19].

4. Establish ethical and governance frameworks. Implementation must include AI ethics, fairness monitoring, and audit logging to prevent bias and ensure public accountability – especially in government financial systems [6,15,17].

5. Foster public–private collaboration. Sharing anonymized fraud typologies and risk indicators between banks and regulators can exponentially increase detection power while maintaining privacy standards [11,19,20].

Looking ahead, the next phase of research should focus on longitudinal econometric assessment of AI's contribution to systemic risk reduction, productivity, and digital trust. Emerging technologies – including federated learning, graph neural networks, and quantum-resistant cryptography – will further enhance the scalability and security of fraud detection systems.

Ultimately, the integration of AI in financial fraud detection is not merely a technical evolution but a paradigm shift in the governance of trust, accountability, and fiscal sustainability.

Its economic efficiency extends beyond direct cost savings – it reshapes the very architecture of modern financial ecosystems, ensuring resilience, transparency, and confidence in both the private and public sectors.

REFERENCES

1. World Bank. *Artificial Intelligence in the Public Sector: Summary Note.* Washington, D.C., 2021. URL: https://documents1.worldbank.org/curated/en/ 746721616045333426/pdf/Artificial-Intelligence-in-the-Public-Sector-Summary-Note.pdf
2. McKinsey & Company. *AI in the Workplace: A Report for 2025.* URL: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work
3. ResearchGate. *AI-driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity.* URL: https://www.researchgate.net/publication/386276951_AI-driven_fraud_detection_in_banking_A_systematic_review_of_data_science_approaches_to_enhancing_cybersecurity
4. Chen, Y. *Deep Learning in Financial Fraud Detection. ScienceDirect.* URL: https://www.sciencedirect.com/science/article/pii/S2666764925000372

5. CatalisGov. *AI Is Reshaping Fraud Detection in Government Payment Systems.* URL: https://catalisgov.com/ai-is-reshaping-fraud-detection-in-government-payment-systems/
6. OECD. *Governing with Artificial Intelligence: AI in Fighting Corruption and Promoting Public Integrity.* URL: https://www.oecd.org/en/publications/2025 /governing-with-artificial-intelligence_398fa287/full-report/
7. Arab Monetary Fund (AMF). *Using Artificial Intelligence (AI) in Banking Services.* URL: https://www.amf.org.ae/sites/default/files/publications/2022-01/ booklet-series-issue-no-24-using-artificial-intelligence-ai-in-banking-services_0.pdf
8. ResearchGate. *Smart Public Finance: Leveraging AI to Optimize Government Expenditures and Investments.* URL: https://www.researchgate.net/publication/392705944_Smart_Public_Finance_Leveraging_AI_to_Optimize_Government_Expenditures_and_Investments
9. CaspianOne. *AI Adoption in Financial Services: 2025 Report.* URL: https://www.caspianone.com/ai-in-financial-services-report
10. Federal Agency for Technical Regulation and Metrology. *GOST R 7.0.5–2008: Bibliographic Reference. General Requirements and Rules.* URL: https://docs.cntd.ru/document/1200063713
11. European Central Bank (ECB). *Item 2B: Artificial Intelligence* (Bond Market Contact Group). URL: https://www.ecb.europa.eu/paym/groups/pdf/bmcg/ 240919/Item_2B_Artificial_Intelligence.pdf
12. International Monetary Fund (IMF). *Understanding Artificial Intelligence in Tax and Customs Administration*. URL: https://www.imf.org/en/ Publications/TNM/Issues/2024/11/21/Understanding-Artificial-Intelligence-in-Tax-and-Customs-Administration-555097
13. Financial Action Task Force (FATF). *AI and Anti-Money Laundering: Challenges and Policy Responses.* URL: https://www.fatf-gafi.org/publications/ai-aml-challenges.html
14. PwC. *Reducing False Positives in Financial Fraud Detection through Hybrid AI Systems.* URL: https://www.pwc.com/gx/en/industries/financial-services/publications/reducing-false-positives-hybrid-ai.html
15. Deloitte Insights. *Economic Impact of False Positives in Financial Compliance.* URL: https://www2.deloitte.com/global/en/insights/industry/ financial-services/false-positive-impact-financial-compliance.html
16. IMF. *AI in Public Finance: Reducing Fraud and Improving Accountability.* URL: https://www.imf.org/en/Publications/REO/Issues/2024/XX
17. ECB. *Artificial Intelligence in Financial Services: Risk Management and Economic Implications.* https://www.ecb.europa.eu/paym/groups/pdf/bmcg/ 240919/Item_2B_Artificial_Intelligence.pdf
18. IMF. *Leveraging AI for Fiscal Transparency and Fraud Prevention in Emerging Markets.* https://www.imf.org/en/Publications/TNM/Issues/2024/11/21/ Understanding-Artificial-Intelligence-in-Tax-and-Customs-Administration-555097
19. FATF. *AI and Anti-Money Laundering: Challenges and Policy Responses.* URL: https://www.fatf-gafi.org/publications/ai-aml-challenges.html
20. PwC. *Reducing False Positives in Financial Fraud Detection through Hybrid AI Systems.* URL: https://www.pwc.com/gx/en/industries/financial-services/publications/reducing-false-positives-hybrid-ai.html