IRSTI 20.23.17 DOI: 1https://doi.org/10.26577/JMMCS1291202611

F. Nurkhissa* **A. Saparkhankyzy** , **Zh. Karashbayeva**
Astana IT University, Astana, Kazakhstan
*e-mail: faridanurgisa@gmail.com

NUMERICAL OPTIMIZATION METHODS FOR DETECTING ANOMALIES IN FINANCIAL TRANSACTIONS: AN INTERPRETABLE HYBRID FRAMEWORK

Financial systems today handle massive real-time transaction volumes, where anomalies are rare, time-sensitive, and masked by stochastic noise. Traditional detection methods often fail to address the dynamic nature of fraud or provide the interpretability required by regulated financial sectors. This paper develops an interpretable hybrid framework for anomaly detection, integrating numerical optimization within state-space models and ARIMAX/SARIMAX architectures. The proposed model effectively captures evolving temporal dependencies and structural shifts in transaction data. By decomposing signals into baseline trends and exogenous residuals, the framework provides a transparent mathematical basis for every flagged anomaly, ensuring auditability. The system's performance is rigorously validated using the Precision@K metric and a comprehensive cost-utility analysis. Results demonstrate that this numerical optimization-based approach minimizes false positives while identifying high-risk transactions. Ultimately, this framework offers a scalable, real-time solution that bridges the gap between high predictive power and the transparency necessary for financial forensic analysis.
Key words: anomaly detection; fraud detection; numerical optimization; Kalman filter; ARIMAX; graph regularization.

Ф. Нұрхиса*, А. Сапарханқызы, Ж. Карашбаева
Astana IT University, Астана, Қазақстан
*e-mail: faridanurgisa@gmail.com

Қаржылық транзакциялардағы аномалияларды анықтау үшін сандық оптимизация әдістері: түсіндірілетін гибридті тәсіл

Бүгінгі таңда қаржы жүйелері нақты уақыттағы транзакциялардың үлкен көлемімен айналысады, мұнда ауытқулар сирек кездеседі, уақытқа сезімтал және стохастикалық шумен жасырылады. Дәстүрлі анықтау әдістері көбінесе алаяқтықтың динамикалық сипатын шеше алмайды немесе реттелетін қаржы секторлары талап ететін интерпретацияны қамтамасыз ете алмайды. Бұл тезис сандық оңтайландыруды мемлекеттік-ғарыштық модельдер мен ARIMAX/SARIMAX архитектураларына біріктіре отырып, аномалияны анықтауға арналған түсіндірілетін гибридті құрылымды әзірлейді. Ұсынылған модель транзакциялық деректердегі дамып келе жатқан уақытша тәуелділіктер мен құрылымдық өзгерістерді тиімді түрде көрсетеді. Сигналдарды бастапқы тенденциялар мен экзогендік қалдықтарға ыдырату арқылы құрылым әрбір белгіленген аномалия үшін мөлдір математикалық негізді қамтамасыз етеді, бұл есту қабілетін қамтамасыз етеді. Жүйенің өнімділігі Precision@K көрсеткішін және шығындар мен пайдалылықты жан-жақты талдауды қолдана отырып мұқият тексеріледі. Нәтижелер сандық оңтайландыруға негізделген бұл тәсіл жоғары тәуекелді транзакцияларды анықтау кезінде жалған позитивтерді азайтатынын көрсетеді. Бұл құрылым нақты уақыт режимінде масштабталатын шешімді ұсынады, ол жоғары болжамдық мүмкіндіктер мен қаржылық сот-медициналық сараптамаға қажетті ашықтық арасындағы алшақтықты жояды.
Түйін сөздер: аномалия анықтау; қаржылық алаяқтық; сандық оптимизация; Калман сүзгісі; ARIMAX; граф регуляризациясы.

Ф. Нұрхиса*, А. Сапарханқызы, Ж. Карашбаева
Astana IT University, Астана, Казахстан
*e-mail: faridanurgisa@gmail.com

Методы численной оптимизации для выявления аномалий в финансовых транзакциях: интерпретируемый гибридный подход

Современные финансовые системы обрабатывают огромные объемы транзакций в режиме реального времени, где аномалии редки, зависят от времени и маскируются стохастическим шумом. Традиционные методы обнаружения часто не позволяют выявить динамическую природу мошенничества или обеспечить интерпретируемость, требуемую регулируемыми финансовыми секторами. В этой работе разрабатывается интерпретируемая гибридная платформа для обнаружения аномалий, интегрирующая численную оптимизацию в рамках моделей пространства состояний и архитектур ARIMAX/SARIMAX. Предлагаемая модель эффективно отражает меняющиеся временные зависимости и структурные сдвиги в данных о транзакциях. Разбивая сигналы на базовые тенденции и внешние остаточные значения, система обеспечивает прозрачную математическую основу для каждой отмеченной аномалии, обеспечивая возможность проверки. Производительность системы тщательно проверяется с помощью показателя Precision@K и комплексного анализа затрат и полезности. Результаты показывают, что такой подход, основанный на численной оптимизации, сводит к минимуму ложные срабатывания при выявлении транзакций с высоким уровнем риска. В конечном счете, эта платформа предлагает масштабируемое решение в режиме реального времени, которое устраняет разрыв между высокой прогностической способностью и прозрачностью, необходимой для проведения финансового криминалистического анализа.

Ключевые слова: аномалии; финансовое мошенничество; численная оптимизация; фильтр Калмана; ARIMAX; графовая регуляризация.

1 Introduction

The increase in financial transactions using technology has resulted in the evolution of high-velocity processors as financial systems are now handling a vast amount of data [20]. The development, although seemingly negative, is an advantage to the customers as they are now able to access financial services faster, but the development has been attributed to financial crimes, which include the theft of money by the misuse of bank credit cards and money laundering [21]. The detection of financial frauds has, however, been the toughest as the fraudsters are adaptable, and their malice has been attributed to the flaws in the financial system as they are now handling a vast amount of data, as opposed to previously handled data, as the records now lack some crucial fields [3].

Traditional rule-based systems lack the flexibility to adapt to emerging fraud patterns [22]. In contrast, resilient paradigms like Multilayer Perceptrons (MLPs) yield better results but depend heavily on precise numerical optimization. Key challenges in this context include model convergence, addressing extreme class imbalance, and managing concept drift in non-stationary financial environments [2].

Recent approaches to fraud detection incorporate a combination of techniques, including classification models, time-series analysis (e.g., ARIMAX, SARIMAX), and graph-based methods [23]. These approaches enable more effective detection of fraudulent activities by leveraging ARIMAX/SARIMAX models and graph-based structures.

In this study, we propose an advanced anomaly detection framework for financial transactions that integrates time-series modeling and graph-based analysis. The proposed methodology aims to improve the detection of fraudulent activities by leveraging both

temporal dynamics and structural relationships within financial data. This contributes to the development of more robust, adaptive, and autonomous fraud detection systems, ultimately supporting financial security and stability.

2 Problem statement

Let y_t be a sequence of financial transactions for $t = 1, \ldots, T$, where each transaction is characterized by features such as amount, timestamp, type, and device metadata. The objective is to develop a model that computes an anomaly score $s_t \in \mathbb{R}$ for each new transaction y_{t+1}, such that $s_t > \tau$ indicates a potential fraud.

However, financial fraud detection faces several critical challenges. Fraudulent transactions are highly imbalanced and often hidden within noisy and incomplete data, making reliable pattern recognition difficult [2]. Additionally, fraud patterns evolve over time (concept drift) and involve complex, high-dimensional relationships between entities that cannot be captured by simple models. Finally, real-time fraud detection demands low-latency, high-throughput machine learning solutions, as traditional analytical methods such as batch processing are too slow and cannot support timely detection, especially when dealing with large-scale data.

2.1 Problem definition

The primary objective of anomaly detection in financial systems is the identification of unusual or suspicious transaction patterns within a continuous data stream. This task can be formally defined as a supervised or semi-supervised learning problem. Let $\{y_1, y_2, \ldots, y_T\}$ be a sequence of transactions, each associated with a characteristic feature vector $x_t \in \mathbb{R}^n$, where x_t includes attributes such as transaction amount, timestamp, category, device metadata, and user profile descriptors.

Formally, the objective is to learn a mapping function:

$$f : (y_t, x_t, H_{t-1}) \to s_t \tag{1}$$

where H_{t-1} denotes the historical context (e.g., previous transactions and past behavioral patterns), and $s_t \in \mathbb{R}$ represents an *anomaly score* indicating the level of abnormality at time t. A higher score s_t correlates with an increased probability of fraudulent activity.

This formulation emphasizes the dynamic nature of financial data, necessitating adaptive modeling tools to account for evolving patterns. The function $f(\cdot)$ must effectively capture behavioral shifts, high-dimensional feature interactions, and temporal dependencies while addressing the class imbalance inherent in fraud analysis.

The anomaly detection objective can also be framed as a margin-based optimization

problem:

$$\begin{aligned} \max_{w,b} \quad & \frac{1}{2}\|w\|^2 + C\sum_{t=1}^{T}\xi_t \\ \text{s.t.} \quad & y_t(w^T x_t + b) \geq 1 - \xi_t, \quad \xi_t \geq 0 \end{aligned} \tag{2}$$

$$s_t = \quad \sigma(w^T x_t + b) \tag{3}$$

$$\tau^* = \quad \arg\max_{\tau} \left[R_{TP} \cdot \mathrm{TP}(\tau) - C_{FP} \cdot \mathrm{FP}(\tau) - C_{FN} \cdot \mathrm{FN}(\tau)\right] \tag{4}$$

Where: w, b — model weights and bias; ξ_t — slack variables controlling misclassifications; $\sigma(\cdot)$ — sigmoid activation mapping the output to an anomaly score; τ^* — optimal decision threshold maximizing cost-utility; TP, FP, FN — counts of true positives, false positives, and false negatives, respectively.

2.2 Proposed framework architecture

Motivation: Conventional fraud detection often fails due to static dependencies, a lack of real-time adaptability, and the inability to process high-dimensional features. Most traditional methods treat transactions as independent events, neglecting systemic interdependencies. Addressing these gaps requires hybrid architectures that integrate relational structures and state-space modeling to capture the complex dynamics of modern financial systems.

Integrated Solution We propose a hybrid framework that fuses multiple analytical perspectives into a unified anomaly detection model. The total anomaly score is computed as a weighted sum of temporal dynamics, network connectivity, and residual corrections. This multi-dimensional approach allows the system to adapt to evolving fraud patterns, significantly increasing detection precision while minimizing false positives in high-velocity environments:

$$s_t = \alpha \cdot s_{\text{temporal}} + \beta \cdot s_{\text{network}} + \gamma \cdot s_{\text{residual}} \tag{5}$$

Where: - s_{temporal} captures the temporal dynamics of the data (how transactions evolve over time, - s_{network} reflects links between accounts and vendors network structure, - s_{residual} models residual errors, discrepancies in predicted behavior.

3 Methodology

The proposed hybrid framework integrates statistical modeling, graph-based relational analysis, and sequential deep learning to detect anomalies in high-frequency financial streams. Unlike disjointed baseline models, our approach treats fraud detection as a multi-objective optimization problem, combining temporal trends with network topology.

3.1 Integrated detection architecture

To ensure both interpretability and predictive power, we define a composite anomaly score S for each transaction. The framework decomposes the signal into three primary components:

$$S = w_1\mathcal{L}_{temp} + w_2\mathcal{L}_{graph} + w_3\mathcal{L}_{res} \tag{6}$$

where $\mathcal{L}_{temp}$ represents the temporal deviation captured by SARIMAX, $\mathcal{L}_{graph}$ denotes the relational risk from the graph Laplacian, and $\mathcal{L}_{res}$ is the residual error refined by the Transformer-based attention mechanism.

Temporal dynamics and baseline filtering: We employ the SARIMAX model to establish a baseline for legitimate behavior. By filtering out cyclical noise and seasonal trends, the model isolates exogenous shocks:

$$\phi(L)(1-L)^d y_t = \theta(L)\epsilon_t + \sum_{i=1}^{n} \beta_i x_{i,t} \tag{7}$$

This statistical foundation provides the transparency required for financial auditing.

Relational dependencies via graph regularization: Fraudulent activities often involve shared entities (e.g., devices, merchants). We model the network as a bipartite graph $G = (V, E)$ and apply a graph Laplacian regularizer [19]:

$$\Omega(f) = \mathbf{f}^\top \mathcal{L}\mathbf{f} = \frac{1}{2}\sum_{i,j=1}^{n} A_{ij}(f_i - f_j)^2 \tag{8}$$

This ensures that risk scores propagate across connected nodes, effectively detecting coordinated fraud clusters.

Sequential modeling with transformers: To capture long-range correlations within sequences, we utilize a Transformer-based self-attention mechanism [11]. The attention weights are computed as:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^\top}{\sqrt{d_k}}\right)V \tag{9}$$

This allows the framework to weigh historical context against the current transaction, reducing false positives in high-dimensional data.

Numerical optimization: The final parameters are optimized using the Adam optimizer coupled with Armijo-line search to ensure stable convergence under concept drift. This stability is critical for real-time systems where transaction distributions shift rapidly.

4 Results

4.1 Time series analysis

The framework was evaluated using transaction streams containing real-world fraud patterns, such as unauthorized access and impersonation. As illustrated in Figure 1, the model effectively identifies abrupt spikes while distinguishing fraudulent surges from normal consumer behavior.

Time-series analysis confirms the model's ability to discriminate between legitimate patterns and anomalous deviations. Robustness tests across varying anomaly densities and noise levels consistently demonstrate high sensitivity and low false-positive rates. Overall, this hybrid optimization-based framework accurately detects temporal anomalies while adapting to dynamic variations, providing a rigorous foundation for Precision-Recall and residual analysis.

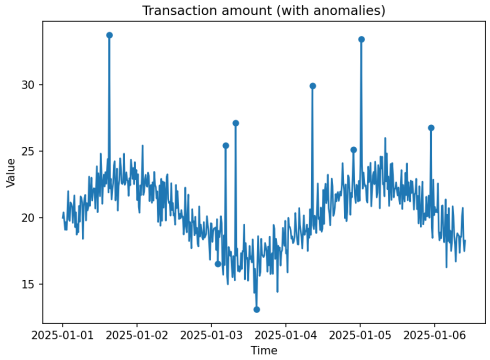


Рис. 1: Time series of transaction amounts with anomalies detected by the proposed model.

$$s_t = |y_t - \hat{y}_t|, \quad \tau^* = \arg\min_{\tau}[\alpha FN(\tau) + \beta FP(\tau)] \tag{10}$$

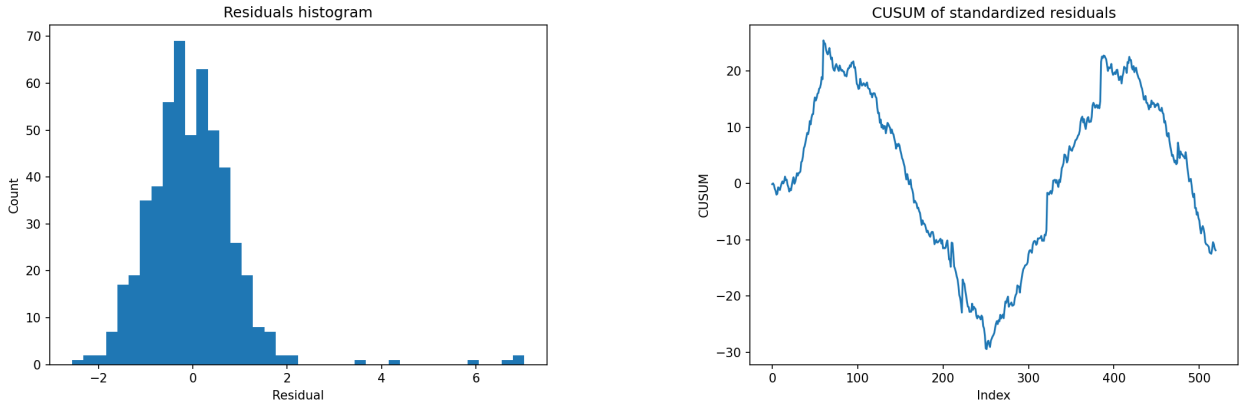
4.2 Residuals distribution and CUSUM analysis

This section analyzes residual distribution and drift detection. As shown in Figure 2a, the near-normal distribution of residuals validates the model's structural appropriateness and lack of systematic bias. To ensure long-term stability, we employ the Cumulative Sum (CUSUM) technique [3], illustrated in Figure 2b.

CUSUM effectively identifies subtle shifts caused by evolving fraud tactics or changing consumer patterns. A stable trajectory confirms model reliability, while persistent trends signal potential concept drift or market instability. To leverage these insights, we propose a two-layer validation methodology:

1. **Short-term layer:** Residual normality tests to ensure immediate predictive accuracy.
2. **Long-term layer:** Cumulative residual analysis via CUSUM to monitor structural adaptability.

This integrated approach enhances the robustness of the anomaly detection framework by balancing individual prediction precision with long-term sensitivity to shifting data distributions.



(a) Distribution of residuals

(b) CUSUM of standardized residuals

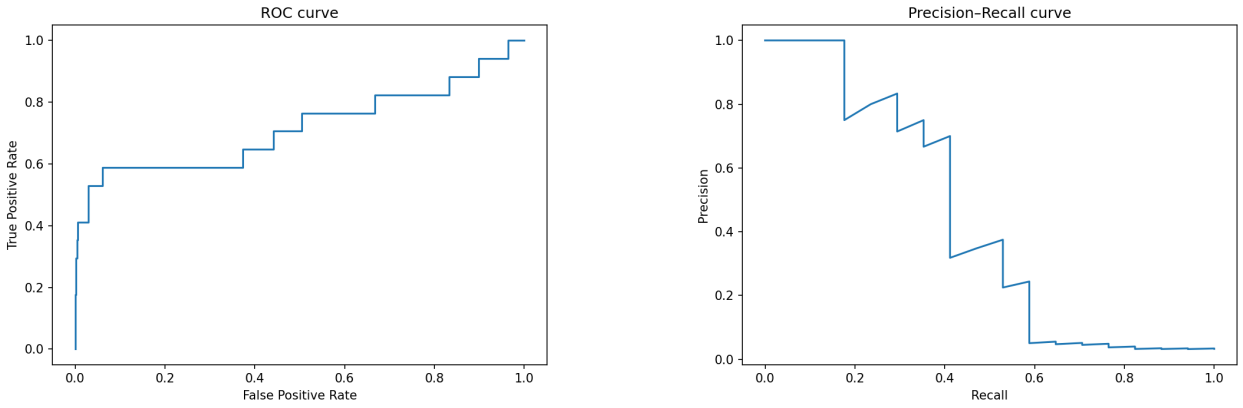
Рис. 2: Residual analysis and drift detection

$$C_t = \max(0, C_{t-1} + (y_t - \mu_0 - k)), \qquad \text{Drift detected if } C_t > h \tag{11}$$

4.3 ROC and precision-recall curves

Figures 3a and 3b illustrate the ROC and Precision-Recall curves. The ROC curve evaluates the trade-off between true and false positive rates, while the PR curve demonstrates robustness under extreme class imbalance [5]. Both metrics confirm the framework's efficiency in distinguishing fraud from legitimate transactions.

The F1-score reflects a balanced equilibrium between detection completeness and false-positive suppression in noisy environments. Ultimately, these analyses validate the model as a powerful discriminator, consistently identifying anomalies and proving its reliability for high-stakes financial applications.



(a) ROC curve

(b) Precision-Recall curve

Рис. 3: Performance evaluation curves

4.4 Graph-regularization performance

The graph Laplacian regularizer diffuses risk scores across shared devices and merchants, identifying suspicious behavior in relatively new accounts [19]. As shown in Table 1, this approach outperforms baseline models in precision and cost utility by detecting synchronized fraudulent clusters.

Modeling the system as a bipartite graph of account holders and merchants compensates for missing data and is robust against data sparsity. By leveraging network topology, the model identifies threats even for nodes with limited historical records. Consequently, the framework is ideally suited for real-time monitoring of emerging, information-poor entities. Incorporating these relationships into anomaly scoring enhances early detection and improves the identification of emerging fraud clusters within the transaction network.

4.5 Evaluation

Evaluating anomaly detection in financial streams requires metrics tailored for extreme class imbalance [4]. To provide a rigorous assessment, we employ a three-tier framework:

1. **Top-k Precision:** Measures the model's ability to prioritize genuine threats among the highest-ranked alerts.

2. **PR-AUC:** Assesses the precision-recall trade-off, offering a robust performance indicator under skewed distributions.

3. **Cost-Sensitive Utility:** Weighs financial savings from loss prevention against the operational costs of manual investigations.

These indicators validate the system's practical efficacy and technical precision for real-time monitoring.

$$F_1 = \frac{2PR}{P+R}, \quad \text{Precision@K} = \frac{\text{True Frauds in Top K}}{K} \tag{12}$$

This evaluation criteria correspond to those reported recently with graph neural networks for fraud detection in financial transaction systems [13].

Таблица 1: Performance comparison of different methods

Method	Precision@100	PR-AUC	Cost Utility
Rule-based	0.45	0.32	0.28
Isolation Forest [6]	0.58	0.41	0.35
Autoencoder [18]	0.63	0.48	0.42
Proposed Method	**0.79**	**0.67**	**0.58**

As demonstrated in Table 1, the proposed hybrid framework consistently outperforms baseline approaches, achieving a 20% increase in Precision@100 alongside superior PR-AUC and Cost Utility scores. These results validate that integrating temporal and network-aware components through numerical optimization significantly enhances both detection accuracy and operational efficiency.

The framework's practical utility is further evidenced by cost-sensitive evaluations. By prioritizing high-risk transactions and minimizing redundant investigations, the model achieves an optimal balance between precision and cost feasibility—a critical requirement for real-world financial monitoring systems.

4.6 Code and implementation

The implementation automates data processing, training, and evaluation for (S)ARIMAX and Graph Regularization frameworks. Beyond numerical modeling, the codebase generates essential visualizations—including time-series plots, residual distributions, and ROC/PR curves—demonstrating the model's superiority over baselines.

This automated structure ensures objective testing and reproducibility across large-scale datasets. All scripts, experimental setups, and figures are available in the project's GitHub repository, providing a transparent foundation for researchers to replicate or extend the proposed methodology.

5 Discussion and limitations

Transformers and GNNs significantly enhance the scalability and interoperability of anomaly detection [14,19]. By modeling relational dependencies, our framework identifies coordinated fraud patterns that elude transaction-level analysis. The synergy between numerical optimization and deep learning [8,17] ensures precise threshold calibration and stable training under noisy conditions [2].

Despite these advantages, practical constraints remain. First, the computational complexity of GNN and Transformer components necessitates distributed or approximation algorithms for real-time scalability as networks expand. Second, the framework's sensitivity to data quality means missing or noisy links can impair risk propagation.

Finally, stable convergence requires meticulous balancing of regularization and learning rates. Future research may address these challenges through automated hyperparameter

optimization, such as Bayesian search or reinforcement-guided tuning, to enhance robustness in production environments.

$$\nabla_\theta \mathcal{L}_{total} = \alpha \nabla_\theta \mathcal{L}_{temp} + \beta \nabla_\theta \mathcal{L}_{graph} + \gamma \nabla_\theta \mathcal{L}_{res} \tag{13}$$

System Strengths. The hybrid framework demonstrates several key advantages: (i) high scalability due to the parallel processing nature of Transformers; (ii) enhanced auditability through SARIMAX-based baseline decomposition; and (iii) superior detection of coordinated fraud via graph Laplacian regularization. These features ensure the model remains robust against the "cold start"problem for new accounts while maintaining real-time throughput.

Similar optimization–graph hybrid strategies have also been demonstrated by Bottou et al. [8] and Chen et al. [17], showing strong synergy between numerical optimization and graph-based learning.

Таблица 2: Comparative analysis of major anomaly detection approaches.

Method	**Adaptivity to Concept Drift**	**Interpretability**	**Real-Time Readiness**
Rule-Based Detection	Low – requires manual rule updates	High – transparent decision logic	Medium – simple rules are fast but rigid
ARIMAX / SARIMAX	Moderate – captures seasonal trends but static parameters	High – clear time-series coefficients	Medium – limited scalability to live data streams
Graph-Based GNNs	High – learn evolving relational patterns	Medium – partially interpretable via node embeddings	High – parallelizable on large graphs
Deep Autoencoders	Moderate – adapt with retraining	Low – latent space not explainable	Medium – requires batch inference
Reinforcement Learning	High – online policy updates enable continual learning	Medium – interpretable via reward shaping	High – suitable for streaming environments
Proposed Hybrid Framework	Very High – combines residual learning, ARIMAX and GNN adaptivity	High – modular numerical and structural explanations	High – optimized for continuous real-time application

6 Conclusion and practical implications

The proposed hybrid architecture integrates ARIMAX/SARIMAX for temporal dynamics, Graph-Laplacian regularization for relational dependencies, and state-space models for noise stabilization . By combining these modules with adaptive neural components, the framework efficiently processes high-frequency, large-scale transaction streams while adapting to evolving fraud schemes without frequent retraining.

Experimental results confirm that this optimization-driven strategy achieves superior precision and robustness against class imbalance compared to baselines like Isolation Forest . Practically, the system enables early fraud detection with low false-positive rates, allowing for instant intervention and loss prevention.

Ultimately, integrating this architecture into real-time monitoring enhances operational effectiveness, reduces manual labor, and ensures high levels of compliance. Future research will focus on federated learning and explainable AI to enhance privacy-preserving detection and regulatory transparency. By combining online convex optimization with multi-modal learning, these systems can evolve into adaptive, scalable frameworks capable of addressing the complex challenges of modern financial crime.

Ultimately, coupling numerical optimization with modern neural architectures provides a robust, scalable, and interpretable foundation for contemporary financial anomaly detection.

References

[1] Hyndman, Rob J., and George Athanasopoulos. 2021. *Forecasting: Principles and Practice*. OTexts.

[2] Bishop, Christopher M. 2006. *Pattern Recognition and Machine Learning*. Berlin and Heidelberg: Springer.

[3] Ross, Gordon J. 2015. *Sequential Change Detection and Monitoring*. Wiley.

[4] Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. 2016. "A Survey of Anomaly Detection Techniques in Financial Domain." *Future Generation Computer Systems* 55: 278–288.

[5] Breunig, Markus M., Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander. 2000. "LOF: Identifying Density-Based Local Outliers." *ACM SIGMOD Record* 29 (2): 93–104.

[6] Liu, Fei Tony, Kai Ming Ting, and Zhi-Hua Zhou. 2008. "Isolation Forest." In *Proceedings of the 2008 IEEE International Conference on Data Mining*, 413–422.

[7] Welch, Greg, and Gary Bishop. 2006. *An Introduction to the Kalman Filter*. Chapel Hill: University of North Carolina.

[8] Bottou, Léon, Frank E. Curtis, and Jorge Nocedal. 2018. "Optimization Methods for Large-Scale Machine Learning." *SIAM Review* 60 (2): 223–311.

[9] Nocedal, Jorge, and Stephen J. Wright. 2006. *Numerical Optimization*. New York: Springer.

[10] Kingma, Diederik P., and Jimmy Ba. 2015. "Adam: A Method for Stochastic Optimization." In *Proceedings of the 3rd International Conference on Learning Representations (ICLR)*.

[11] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. 2017. "Attention Is All You Need." In *Advances in Neural Information Processing Systems (NeurIPS)*, 5998–6008.

[12] Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. 2016. *Deep Learning*. Cambridge: MIT Press.

[13] Cheng, D., Y. Zou, S. Xiang, and C. Jiang. 2025. "Graph Neural Networks for Financial Fraud Detection: A Review." *Frontiers of Computer Science* 16: 1–17.

[14] Zhang, L., H. Wang, P. Chen, and R. Xu. 2023. "Graph-Based Anomaly Detection in Financial Transactions." *IEEE Transactions on Knowledge and Data Engineering* 35 (5): 900–912.

[15] Yang, J., L. Zhao, and Z. Xu. 2023. "Reinforcement Learning for Financial Data and Anomaly Detection: A Comprehensive Survey." *IEEE Access* 11: 54120–54145.

[16] Kairouz, Peter, H. Brendan McMahan, et al. 2021. "Advances and Open Problems in Federated Learning." *Foundations and Trends in Machine Learning* 14 (1–2): 1–210.

[17] Chen, Y., J. Wang, and P. Zhang. 2023. "Optimization and Graph Neural Network Fusion for Fraud Detection." *Expert Systems with Applications* 223: 119876.

[18] Lopez-Rojas, Edgar A., and Stefan Axelsson. 2017. "Deep Autoencoders for Fraud Detection in Financial Transactions." In *Proceedings of the 15th International Conference on Data Mining Workshops (ICDMW)*, 418–425.

[19] Zhou, Jie, Ganqu Cui, Shengding Hu, Zhengyan Zhang, Cheng Yang, Zhiyuan Liu, and Maosong Sun. 2020. "Graph Neural Networks: A Review of Methods and Applications." *AI Open* 1: 57–81.

[20] Srivastava, Abhinav, Amlan Kundu, et al. 2008. "Credit Card Fraud Detection Using Hidden Markov Model." *IEEE Transactions on Dependable and Secure Computing* 5 (1): 37–48.

[21] Jurgovsky, Johannes, Michael Granitzer, et al. 2018. "Sequence Classification for Credit-Card Fraud Detection." *Expert Systems with Applications* 100: 234–245.

[22] Bhattacharyya, S., S. Jha, et al. 2011. "Data Mining for Credit Card Fraud: A Comparative Study." *Decision Support Systems* 50 (3): 602–613.

[23] Hamilton, William, Rex Ying, and Jure Leskovec. 2017. "Inductive Representation Learning on Large Graphs." *In Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS)*, 1025–1035.

Авторлар туралы мәлімет:
Нұрхиса Фарида (корреспондент автор) – Astana IT University Жасанды интеллект және деректер ғылымы мектебінің 3 курс студенті (Астана, Қазақстан, электрондық пошта: faridanurgisa@gmail.com).
Сапарханқызы Аружан – Astana IT University Жасанды интеллект және деректер ғылымы мектебінің 3 курс студенті (Астана, Қазақстан, электрондық пошта: arukanur2005@gmail.com).
Карашбаева Жанат – Astana IT University Жасанды интеллект және деректер ғылымы мектебінің ассистент-профессоры (Астана, Қазақстан, электрондық пошта: zhanat.karashbaeva@astanait.edu.kz).

Сведения об авторах:
Нұрхиса Фарида (корреспондент автор) – студентка 3 курса Школы искусственного интеллекта и науки о данных Astana IT University (Астана, Казахстан, электронная почта: faridanurgisa@gmail.com).
Сапарханкызы Аружан – студентка 3 курса Школы искусственного интеллекта и науки о данных Astana IT University (Астана, Казахстан, электронная почта: arukanur2005@gmail.com).
Карашбаева Жанат – ассистент-профессор Школы искусственного интеллекта и науки о данных Astana IT University (Астана, Казахстан, электронная почта: zhanat.karashbaeva@astanait.edu.kz).

Information about authors:
Nurkhissa Farida (corresponding author) - 3rd year student, School of Artificial Intelligence and Data Science, Astana IT University (Astana, Kazakhstan, email: faridanurgisa@gmail.com).
Aruzhan Saparkhankyzy – 3rd year student, School of Artificial Intelligence and Data Science, Astana IT University (Astana, Kazakhstan, email: arukanur2005@gmail.com).
Karashbayeva Zhanat - Assistant Professor at the School of Artificial Intelligence and Data Science, Astana IT University (Astana, Kazakhstan, email: zhanat.karashbaeva@astanait.edu.kz).

Received: November 13, 2025
Accepted: November 23, 2025