

IMPROVING LEGAL MECHANISMS FOR DETECTING CYBERCRIMES BASED ON STATISTICAL ANALYSIS OF FINANCIAL TRANSACTIONS IN THE BANKING SYSTEM

Akmalbek Abdusalomov^{1,2} and Dilshodjon Egamberdiev^{2,*}

Akmalbek Bobomirzaevich Abdusalomov, Professor of Artificial Intelligence Department, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Tashkent 100200, Uzbekistan, akmalbekabdusalomov@gmail.com

²Akmalbek Abdusalomov, Master Student of Cyber Law Department, Tashkent, State University of Law, Amir Temur Avenue 13, 100000, Tashkent, Uzbekistan, akmalbekabdusalomov@gmail.com

²Dilshodjon Egamberdiev, Professor of Cyber Law Department, Tashkent, State University of Law, Amir Temur Avenue 13, 100000, Tashkent, Uzbekistan, d.egamberdiyev@tsul.uz

Abstract

The rapid expansion of digital banking has significantly increased the scale and complexity of cyber-enabled financial crimes. Traditional legal mechanisms often struggle to keep pace with evolving fraud patterns, particularly in real-time transaction environments. This paper proposes an integrated approach that combines statistical analysis of financial transactions with compliance-aware artificial intelligence to enhance cybercrime detection and legal accountability. By leveraging short-term behavioral patterns, anomaly detection, and regulatory-aligned decision frameworks, the study demonstrates how financial institutions can improve both detection accuracy and legal traceability. The findings highlight the importance of embedding explainability, auditability, and statistical evidence into cybercrime detection systems to support effective law enforcement and regulatory compliance.

Keywords: card-not-present transactions, compliance aware, regulatory framework, fraud detection, artificial intelligence

1. Introduction

The rapid digitalization of banking systems has fundamentally transformed the financial ecosystem by enabling high-frequency, real-time, and cross-border transactions. While these developments have significantly improved efficiency and accessibility, they have also introduced new vulnerabilities that are actively exploited by cybercriminals [1,2]. In particular, card-not-present (CNP) transactions and online payment systems have emerged as critical risk domains due to the absence of physical verification mechanisms. Fraudsters increasingly employ advanced techniques such as phishing, credential stuffing, synthetic identity fraud, and automated bot attacks to bypass traditional security controls [3].

From a legal perspective, cybercrime detection has evolved from a purely technical function into a regulated and compliance-driven obligation. Financial institutions are required not only to detect suspicious transactions but also to ensure that such detections are explainable, auditable, and aligned with regulatory frameworks, including anti-money laundering (AML) policies and cybersecurity regulations [4]. These frameworks impose strict requirements on transparency, data governance, and accountability, particularly in the context of automated decision-making systems.

However, despite substantial progress in both legal regulation and fraud detection technologies, a significant gap remains between traditional legal mechanisms and the dynamic nature of modern cybercrime. Existing legal approaches primarily rely on post-event investigation and forensic analysis, whereas contemporary financial fraud operates in real time and requires

immediate detection supported by statistically grounded evidence. This discrepancy limits the effectiveness of current legal enforcement and delays timely intervention [5].

To address this challenge, this paper proposes a statistical and legally compliant framework for detecting cybercrimes in banking systems. The proposed approach integrates real-time statistical analysis of financial transactions with compliance-aware detection mechanisms, aiming to enhance detection accuracy while ensuring legal interpretability and regulatory alignment.

2. Proposed Approach (Main part)

This study proposes a legal–statistical framework for improving cybercrime detection in banking systems by integrating statistical transaction analysis with regulatory compliance and explainable decision-making mechanisms. The framework is structured around three interrelated components that jointly address the limitations of traditional fraud detection systems, particularly in terms of real-time processing, legal interpretability, and evidentiary validity.

2.1. Statistical Analysis of Transaction Behavior

The first component focuses on the statistical analysis of transaction behavior using short-term temporal windows rather than long-term historical profiles. This approach is motivated by the observation that modern cyber fraud often manifests as rapid, localized anomalies within short time intervals, such as sudden bursts in transaction frequency, irregular timing patterns, and abnormal transaction value deviations [3,6]. By modeling these micro-patterns, the system can capture early indicators of fraudulent activity without relying on extensive historical data, which is often constrained by privacy regulations and data governance requirements. In particular, statistical features such as inter-transaction time gaps, frequency distributions, and value dispersion metrics are extracted and analyzed to identify deviations from normal behavioral baselines. This enables efficient real-time detection with reduced computational overhead while ensuring compliance with data minimization principles imposed by regulations such as GDPR [7]. Consequently, the proposed statistical layer not only enhances detection speed but also aligns with legal constraints on data usage and storage.

2.2. Compliance-Aware Detection Model

The second component introduces a compliance-aware detection model that integrates statistical anomaly detection with formal regulatory rules, including anti-money laundering (AML) requirements and transaction monitoring policies. Unlike conventional machine learning models that operate as black-box predictors, the proposed approach embeds regulatory logic directly into the detection process, ensuring that model outputs are consistent with legal standards [5,6].

This hybrid mechanism combines data-driven anomaly scores with rule-based indicators, such as transaction thresholds, velocity constraints, and jurisdictional risk factors. As a result, each detection decision is supported not only by statistical evidence but also by explicit regulatory justification. This dual-layer design enhances the reliability and legal admissibility of the system by ensuring that outputs can be interpreted and validated within existing legal frameworks. Furthermore, it facilitates integration with reporting mechanisms such as Suspicious Activity Reports (SARs), which require structured and explainable evidence for regulatory and investigative purposes [7].

2.3. Explainable and Auditable Decision Mechanism

The third component focuses on the development of an explainable and auditable decision mechanism that transforms detection outputs into structured legal evidence. A key innovation of

the proposed framework is the generation of comprehensive decision records that include risk probability scores, statistical deviation indicators, and rule-based triggers. These elements collectively provide a transparent representation of the reasoning behind each detection outcome [8].

Such structured outputs enable full traceability of decisions, allowing auditors and investigators to reconstruct the decision-making process and verify its compliance with regulatory requirements. In addition, the integration of explainability mechanisms ensures that the system satisfies legal expectations for transparency and accountability in automated decision-making systems [9]. This is particularly important in high-stakes financial environments, where decisions may be subject to legal scrutiny and must be admissible as digital evidence in judicial or regulatory proceedings.

Overall, the proposed framework bridges the gap between statistical fraud detection and legal enforcement by providing a unified approach that ensures real-time performance, regulatory alignment, and evidentiary robustness.

3. Results, Discussion and Legal Implications

The experimental evaluation conducted on large-scale banking transaction data demonstrates that the proposed legal–statistical framework significantly improves the effectiveness of cybercrime detection in financial systems. In particular, statistical pattern-based analysis, which focuses on short-term transactional behavior, enables the identification of fraud-related anomalies with higher precision compared to traditional approaches [3-6]. The use of micro-patterns such as transaction frequency bursts, temporal irregularities, and value deviations allows the system to detect suspicious activities at early stages, thereby enhancing overall fraud identification performance. Furthermore, the proposed framework satisfies strict real-time processing requirements typical for modern banking environments. By reducing reliance on long-term historical data and employing computationally efficient statistical features, the system achieves low-latency decision-making while maintaining high detection accuracy [8]. This is particularly important in payment authorization systems, where decisions must be made within milliseconds.

A key advantage of the framework lies in the integration of legal and regulatory rules into the detection process. The inclusion of compliance-aware mechanisms, such as AML-based transaction monitoring and rule-driven validation, significantly reduces false positive rates and improves the reliability of detection outcomes [8,9]. Unlike conventional machine learning models that operate as opaque “black-box” systems, the proposed approach provides structured and interpretable outputs that combine statistical evidence with regulatory justification [10]. Importantly, the system generates quantifiable and reproducible decision evidence, including risk probability scores, anomaly indicators, and rule-based triggers. This ensures that each detection can be systematically reconstructed and verified, which is critical for legal proceedings and regulatory audits [11]. The ability to produce audit-ready outputs addresses a major limitation of traditional AI-based fraud detection systems, where lack of transparency often hinders legal acceptance and enforcement [12]. From a legal perspective, the proposed framework contributes to strengthening cybercrime detection mechanisms in several ways. First, it enhances evidence generation by ensuring that each detection is supported by both statistical analysis and explicit logical reasoning, enabling the transformation of detection results into legally admissible digital evidence [13]. Second, the framework ensures regulatory compliance, as it aligns detection

processes with existing legal standards, including data protection regulations (e.g., GDPR), anti-money laundering (AML) requirements, and cybersecurity frameworks [10-14]. Third, it supports cross-border applicability, as the structured and standardized nature of decision outputs allows them to be interpreted and utilized across different legal jurisdictions [15].

In addition to these contributions, the findings of this study highlight the necessity of improving existing legal frameworks to fully leverage the capabilities of AI-driven fraud detection systems. Based on the experimental results and identified limitations, several key policy recommendations can be proposed.

First, it is essential to establish legal standards for AI-based decision-making systems, requiring that automated decisions in financial fraud detection be explainable, transparent, and reproducible [14, 15]. Such requirements would ensure that AI-generated outcomes can be validated and accepted within judicial and regulatory contexts.

Second, there is a need to formally define and standardize digital evidence generated by AI systems, including risk scores, anomaly indicators, and rule-based triggers, as legally admissible forms of evidence in cybercrime investigations [6]. This would significantly enhance the role of automated systems in legal proceedings.

Third, regulatory authorities should mandate real-time transaction monitoring and automated reporting mechanisms, such as dynamic Suspicious Activity Reports (SARs), to ensure timely detection and response to cyber threats [11], [8]. This shift from post-event investigation to proactive monitoring is critical in modern digital banking environments.

Fourth, it is necessary to clarify the balance between data minimization and effective fraud detection, ensuring that statistical analysis methods comply with privacy regulations while maintaining sufficient analytical capability [3]. Clear legal guidelines on permissible data usage would reduce uncertainty in AI system deployment.

Finally, strengthening international cooperation and standardization is crucial, as cybercrime in financial systems is inherently cross-border. Developing unified reporting formats, interoperable detection standards, and shared regulatory frameworks would facilitate collaboration between jurisdictions and improve the global effectiveness of cybercrime prevention [4].

Overall, the proposed approach not only improves fraud detection performance but also provides a foundation for aligning technological innovation with legal and regulatory requirements. By integrating statistical analysis, explainable AI, and compliance-aware mechanisms, the framework effectively bridges the gap between technical fraud detection systems and legal enforcement processes [5], [7].

4. Conclusions and Future Directions

This paper showed that improving cybercrime detection in banking systems requires combining statistical analysis with legal requirements, not treating them separately. The proposed framework demonstrates that short-term transaction patterns can effectively detect fraud in real time, while also meeting key legal needs such as transparency, auditability, and compliance. Unlike traditional “black-box” models, this approach produces clear and reproducible results that can be used as legal evidence, helping bridge the gap between technical detection and legal enforcement.

Future work should focus on making these systems more practical and widely applicable. First, there is a need to standardize AI-generated evidence so it can be accepted in courts and across countries. Second, stronger integration with international legal frameworks will be important for handling cross-border cybercrime. Third, improving explainable AI methods will help ensure trust

and regulatory acceptance. In addition, privacy-preserving techniques should be explored to balance data protection with detection performance. Finally, real-world implementation and testing in banking environments will be essential to validate the effectiveness of such systems in practice. Overall, combining statistical methods, AI, and legal mechanisms offers a promising path toward more effective and reliable cybercrime detection in modern financial systems.

References

1. Chen, X.; Li, Y.; Zhang, H. Digital Banking and Cybersecurity Risks in Modern Financial Systems. *Journal of Financial Technology* 2025, 12, 45–60.
2. Baisholan, N.; Kumar, R.; Singh, P. Cyber Fraud Trends and Detection Challenges in Financial Systems. *Computers & Security* 2025, 130, 103245.
3. Motie, S.; Raahemi, B. Fraud Detection in Card-Not-Present Transactions Using Machine Learning Techniques. *Expert Systems with Applications* 2024, 235, 121234.
4. Sturc, L.; Novak, J.; Horvat, M. Regulatory Frameworks for Financial Cybercrime Detection: A Comparative Study. *Journal of Cyber Policy* 2022, 7, 89–105.
5. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union* 2016, L119, 1–88.
6. A. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. Portier, L. He-Guelton, and O. Caelen, “Sequence Classification for Credit-Card Fraud Detection,” *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.
7. L. Sturc, J. Novak, and M. Horvat, “Regulatory Frameworks for Financial Cybercrime Detection: A Comparative Study,” *Journal of Cyber Policy*, vol. 7, no. 1, pp. 89–105, 2022.
8. M. Abdurashidova and M. Balbaa, “Artificial Intelligence in the Banking Sector in Uzbekistan: Exploring the Impacts and Opportunities,” in *Proc. ACM Int. Conf.*, 2023.
9. K. Norbaev, “AI-Based Phishing Detection in Uzbek Language and Banking Systems,” *Journal of Information Security*, 2025.
10. M. Kurbonbekova, “Data-Driven Fraud Detection Framework for Digital Payment Systems in Uzbekistan,” *International Scientific-Technical Journal*, 2025.
11. A. Abdusalomov, A. Kutlimuratov, and C. S. Ogurlu, “A Unified Neural–Symbolic Compliance-Aware Framework for Real-Time Fraud Detection in Regulated Financial Systems,” 2026.
12. Central Bank of the Republic of Uzbekistan, “Cybersecurity and Fraud Prevention in Digital Banking Systems,” Tashkent, 2024.
13. Financial Action Task Force (FATF), “International Standards on Combating Money Laundering and the Financing of Terrorism,” 2023.
14. L. Sturc et al., “Regulatory Frameworks for Financial Cybercrime Detection,” *Journal of Cyber Policy*, 2022.
15. A. Jain et al., “Explainable AI in Financial Fraud Detection,” *IEEE Access*, 2023.