Financial Risk and Management:
An International Journal
Volume 4, Number 1, 2025

ZERA

Fintech-Based Predictive Risk Systems and Their Mitigating Effect on Fraud and Operational Risks

Fais Maulidiana[1]

[1] Universitas Nahdlatul Ulama Surabaya, Surabaya, Indonesia

Abstract

Article history:
Received: January 5, 2025
Revised: February 23, 2025
Accepted: April 3, 2025
Published: June 30, 2025

Keywords:
Fintech,
Fraud Detection,
Operational Risk,
Predictive Risk Systems,
Risk Mitigation.

Identifier:
Zera Open
Page: 56-68
https://zeraopen.com/journal/frmij

This article investigates how fintech-based predictive risk systems contribute to mitigating fraud and operational risks in highly digital and data-driven financial environments. It addresses the question of when and how machine-learning and analytics-driven tools move beyond improving classification metrics to actually reduce realized fraud losses, service disruptions, and compliance failures. The study draws on a systematic review of peer-reviewed articles published between 2020 and 2024 that analyze predictive models embedded in digital payments, e-commerce, platform-based finance, and related fintech services. The reviewed evidence shows that these systems consistently outperform traditional rule-based approaches, particularly when they integrate granular transactional, behavioral, and network data and operate in near real time. Through narrative and thematic synthesis, the article discusses prevailing design patterns, data sources, modelling techniques, and governance practices surrounding these systems. The main findings underline strong technical performance but fragmented governance, limited measurement of loss reductions, and the need for more integrated, proactive risk architectures around fintech-based predictive systems.

1. Introduction

Fintech innovation has transformed how financial services are delivered, but it has also created new exposure to fraud and operational disruptions in highly digital, data intensive environments. Digital payment platforms, peer to peer lending, open banking interfaces, and cloud-based core systems increase the attack surface for cyber fraud, model misuse, and process breakdowns that can quickly propagate across interconnected infrastructures (Bu et al., 2023; Rolando & Mulyono, 2024). At the same time, regulators and boards are demanding more proactive, data driven approaches to risk, moving beyond static rule sets and backward-looking controls toward dynamic, predictive risk systems that operate close to real time. These developments position fintech based predictive analytics as a critical layer in modern fraud and operational risk management architectures.

Recent studies show that machine learning and anomaly detection models embedded in fintech platforms can significantly enhance the detection of fraudulent transactions and abnormal behavioral patterns compared with traditional rule-based systems (Stojanović et al., 2021; Damayanti & Adrianto, 2023). User centered explainable AI frameworks further demonstrate how ensemble predictive models combined with Shapley value-based explanations can deliver both high accuracy and interpretable fraud risk scoring at the level of individual transactions and customers, improving trust and oversight in digital financial services (Zhou et al., 2023). Beyond fraud, predictive analytics is increasingly leveraged to anticipate system outages, process bottlenecks, and compliance breaches, allowing institutions to prioritize controls and interventions before losses materialize (Azubuike, 2024; Rolando &

Mulyono, 2024). However, empirical evidence on how far these systems actually mitigate fraud and operational risk, rather than simply improving detection metrics in experimental settings, remains scattered across domains and technologies.

The academic and practitioner literature on fintech based predictive risk systems is fragmented across multiple streams, including financial fraud detection, operational risk management, RegTech and SupTech, and AI governance in financial institutions. Systematic literature reviews of machine learning based financial fraud detection synthesize evidence on algorithms, datasets, and evaluation metrics, but note that many studies emphasize model performance while devoting less attention to governance mechanisms such as data quality controls, model risk management, human oversight, and regulatory alignment (Ali et al., 2022; Hernandez Aros et al., 2024). Empirical work on risk analytics in fintech similarly underscores the promise of predictive systems, yet offers limited cross comparison of when and how these tools reduce realized fraud losses, operational incidents, and associated costs in live production environments (Zhou et al., 2023; Azubuike, 2024; Rolando & Mulyono, 2024). This gap makes it difficult for decision makers to benchmark alternative architectures and governance arrangements for predictive risk systems.

This article addresses these gaps by conducting a systematic literature review of peer reviewed studies published between 2020 and 2024 on fintech based predictive risk systems and their mitigating effect on fraud and operational risks. The review synthesizes evidence on system designs, data sources, analytical techniques, and implementation contexts, as well as reported impacts on fraud losses, operational incidents, and regulatory compliance outcomes. By integrating findings from finance, information systems, accounting, and risk management journals, the study clarifies how predictive analytics is currently used to manage fraud and operational risks in fintech intensive settings, identifies the governance mechanisms that support effective deployment, and highlights unresolved challenges around bias, explainability, and resilience.

2. Literature Review

The literature on fintech-based predictive risk systems is dominated by studies that apply machine learning to financial fraud detection, with a growing subset addressing broader operational risk. Systematic reviews and survey articles document a rapid expansion of artificial intelligence and machine learning techniques for detecting anomalous or fraudulent behaviour in financial data, including transactional, e-commerce, and banking contexts (Ali et al., 2022; Damayanti & Adrianto, 2023; Hernandez Aros et al., 2024). These studies typically compare supervised and unsupervised algorithms, evaluate performance metrics such as precision and recall, and assess the impact of data imbalance and feature engineering on model accuracy. A key insight from this stream is that machine learning dramatically improves detection performance over traditional rule-based systems, but most contributions remain focused on algorithmic optimization rather than on how predictive systems are embedded into institutional fraud and risk management processes.

A second strand of literature narrows in on fintech-specific applications, particularly digital payments and platform-based financial services, where real-time or near-real-time predictive risk systems are most needed. Empirical work on fintech applications shows that behaviour-based models and ensemble approaches can detect subtle, evolving fraud patterns in high-volume transaction streams, especially when models integrate device, network, and user-behavioural features (Stojanović et al., 2021; Zhou et al., 2023). Systematic reviews of financial fraud detection using machine-learning algorithms highlight the diversity of algorithmic choices and data sources, but also emphasize that many implementations do not adequately consider governance elements such as data quality controls, model risk management, and human oversight (Ali et al., 2022; Husnaningtyas & Dewayanto, 2023). Parallel work in fintech risk and AI-based risk management underlines that predictive analytics is increasingly used for early warning and real-time surveillance, yet the evidence on its effect on realized fraud losses and operational incidents is still fragmented (Bu et al., 2023; Rolando & Mulyono, 2024).

Beyond fraud detection, a growing body of research explores predictive analytics as a broader risk mitigation tool across financial and non-financial industries. Review studies on predictive analytics applications for risk mitigation argue that predictive models can support proactive management of operational, compliance, and process risks by identifying early warning signals, forecasting incident likelihood, and guiding the allocation of control resources (Azubuike, 2024; Valli, 2024). In related work on fintech, financial reporting, and audit, emerging technologies such as blockchain, artificial intelligence, and the Internet of Things are shown to enhance fraud prevention and safeguard equity investments by improving information reliability and transaction traceability (Roszkowska, 2021). However, these studies also stress persistent challenges related to data governance, model interpretability, and the integration of predictive systems with broader risk and control frameworks. Overall, the literature suggests that while fintech-based predictive risk systems hold substantial promise for mitigating fraud and operational risks, their effectiveness depends on how they are governed, monitored, and integrated into organizational risk architectures.

3. Methods

This study uses a systematic literature review approach to synthesize current evidence on fintech based predictive risk systems and their mitigating effect on fraud and operational risks. The review focuses on peer reviewed journal articles published between 2020 and 2024 to capture the most recent wave of fintech, machine learning, and predictive analytics applications in fraud and operational risk management. Relevant studies were identified through structured keyword searches in major academic databases such as Scopus, Web of Science, ScienceDirect, and Google Scholar, using combinations of terms including "fintech", "predictive analytics", "machine learning", "fraud detection", "operational risk", "early warning", and "risk prediction". The search was limited to English language articles. Conference papers, theses, book chapters, non peer-reviewed materials, and purely technical papers without any clear focus on fraud or operational risk mitigation were excluded. Reference lists of key articles were also screened to identify additional eligible studies.

A multi stage screening procedure was applied to refine the initial pool of records. First, titles and abstracts were reviewed to exclude studies that did not involve fintech based or data driven predictive systems, or that did not address fraud, operational risk, or closely related risk categories such as compliance and process risk. Second, full text screening was used to retain empirical, conceptual, and review papers that explicitly examined how predictive models are designed, implemented, or evaluated in the context of fraud or operational risk management in financial and fintech settings. The final set of studies was coded using a structured template that captured publication details, type of fintech or financial service, data sources, analytical techniques, risk types, and reported impacts on fraud or operational risk outcomes. Given the diversity of methods, technologies, and contexts, the evidence was synthesized using a narrative and thematic approach rather than quantitative meta-analysis, with the aim of identifying common design patterns, governance mechanisms, and gaps in the existing literature.

4. Results and Discussion

The review findings show that fintech-based predictive risk systems are most mature in fraud detection, particularly in high-volume payment and e-commerce environments. Across the sampled studies, machine-learning models such as random forests, gradient boosting, and deep neural networks consistently outperform traditional rule-based and statistical approaches in identifying anomalous or fraudulent transactions, especially under severe class imbalance (Stojanović et al., 2021; Ali et al., 2022; Hernandez Aros et al., 2024). Many implementations exploit rich feature spaces that combine transactional attributes, device and network metadata, and behavioural signals, allowing models to capture subtle patterns associated with account takeover, synthetic identities, or collusive fraud (Zhou et al., 2023). Empirical evidence indicates that these systems achieve higher precision and recall, lower false-positive rates, and faster detection times, which directly support fraud risk mitigation and operational efficiency in fintech platforms (Damayanti & Adrianto, 2023; Husnaningtyas & Dewayanto, 2023).

The evidence also points to a gradual expansion of predictive systems beyond pure fraud detection toward broader operational and compliance risk management. Studies on fintech and banking risk early-warning mechanisms show that predictive models are used to flag deteriorating risk profiles in credit portfolios, payment flows, and platform-level indicators, often via time-series forecasting and regime-switching or vector autoregressive frameworks (Bu et al., 2023; Rolando & Mulyono, 2024). In the context of payments and tokenization, AI-enabled risk detection frameworks link real-time anomaly detection with regulatory requirements such as the payment card industry data security standard (PCI-DSS) and the revised payment services directive (PSD2), thereby simultaneously addressing fraud and compliance risk (Mahajan, 2024). These systems embed predictive analytics into continuous monitoring of key risk indicators, automating incident prioritization and enabling faster remediation, which contributes to mitigating operational breakdowns and regulatory breaches.

Another important result concerns the way predictive analytics is used to support proactive rather than reactive risk management. Evidence from fintech lending and investment shows that predictive analytics is increasingly applied to anticipate credit defaults, liquidity stress, and portfolio deterioration, allowing firms to adjust underwriting standards, exposure limits, or pricing before losses materialize (Azubuike, 2024; Tsapa, 2024). Cross-sector reviews of predictive analytics argue that similar techniques can be extended to process and compliance risks, for example by forecasting incident likelihood or control failures and reallocating resources toward high-risk processes (Valli, 2024). In cybersecurity-focused fintech contexts, predictive models built on big data and machine learning are deployed to generate cyber threat intelligence, detect emerging attack patterns, and harden digital financial infrastructures, thereby reducing the probability and impact of operational disruptions (Ekundayo et al., 2024). Together, these studies suggest that fintech-based predictive systems can meaningfully reduce both fraud losses and operational incidents when integrated into forward-looking risk processes.

At the same time, the review highlights significant heterogeneity in governance, explainability, and organizational readiness for these systems. Several studies emphasize that the risk-mitigating effect of predictive systems depends on data governance, model risk management, and the design of human oversight, including how alerts are triaged and how model outputs are embedded into decision workflows (Roszkowska, 2021; Ali et al., 2022). Recent work on AI-enabled risk detection and compliance governance in fintech portfolios shows that organizations with more advanced AI governance and maturity models achieve larger gains in fraud detection speed, loss forecasting accuracy, and compliance cost reduction, underscoring the importance of structured governance frameworks for operational resilience (Mahajan, 2024). However, many empirical contributions still report only technical performance metrics and do not provide robust evidence on realized financial loss reductions, near-miss prevention, or long-term operational risk outcomes. This gap indicates that future research should more systematically link predictive model performance to measurable fraud and operational risk mitigation, while also examining ethical, interpretability, and regulatory dimensions of large-scale deployment in fintech ecosystems.

5. Conclusion

The review concludes that fintech-based predictive risk systems have become a central component of modern fraud and operational risk management, but their development is uneven across domains and institutions. Machine-learning and anomaly detection models embedded in digital payments, e-commerce, and platform-based financial services consistently outperform traditional rule-based systems in detecting fraudulent and anomalous behaviour. When combined with rich transactional, behavioural, and network data, these systems can improve detection accuracy, reduce false positives, and shorten response times, thereby supporting a tangible mitigating effect on fraud and some dimensions of operational risk.

At the same time, the evidence shows that the transition from reactive to proactive risk management is still incomplete. Predictive analytics is increasingly used for early-warning, continuous monitoring, and forecasting of credit, process, and compliance risks, but many studies remain focused on technical performance metrics rather than on realized reductions in losses, incidents, or regulatory breaches.

Governance aspects such as data quality management, model risk control, explainability, and human oversight are often mentioned but less frequently operationalized or evaluated. This creates a gap between the technical promise of predictive systems and their demonstrable contribution to overall fraud and operational risk mitigation.

These findings suggest several implications for practice and research. Financial institutions and fintech firms need to embed predictive models within robust risk architectures that integrate data governance, model validation, and clear escalation and decision workflows, rather than treating predictive engines as standalone tools. Regulators and supervisors, in turn, can play a role by clarifying expectations around explainability, accountability, and evidence of risk reduction for AI-driven risk systems. Future research should move beyond algorithmic comparisons to examine how specific configurations of technology, governance mechanisms, and organizational capabilities influence measurable fraud and operational risk outcomes in real-world fintech environments.

References

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637.

Azubuike, J. I. (2024). The role of predictive analytics in automating risk management and regulatory compliance in the US financial sector. *European Journal of Accounting, Auditing and Finance Research, 12*(10), 19-31.

Bu, Y., Du, X., Li, H., Yu, X., & Wang, Y. (2023). Research on the FinTech risk early warning based on the MS-VAR model: An empirical analysis in China. *Global Finance Journal, 58*, 100898.

Damayanti, R., & Adrianto, Z. (2023). Machine learning for e-commerce fraud detection: A systematic literature review. *Jurnal Riset Akuntansi dan Bisnis Airlangga, 8*(2), 1562–1577.

Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive analytics for cyber threat intelligence in fintech using big data and machine learning. *International Journal of Research Publication and Reviews, 5*(11), 5934–5948.

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications, 11*(1), 1130.

Husnaningtyas, N., & Dewayanto, T. (2023). Financial fraud detection and machine learning algorithm (unsupervised learning): Systematic literature review. *Jurnal Riset Akuntansi dan Bisnis Airlangga, 8*(2), 1521–1542.

Mahajan, N. (2024). AI-Enabled Risk Detection and Compliance Governance in Fintech Portfolio Operations. *Cuestiones de Fisioterapia, 53*(03), 5366-5381.

Rolando, B., & Mulyono, H. (2024). Managing Risks In Fintech: Applications And Challenges Of Artificial Intelligence-Based Risk Management. *Economics and Business Journal (ECBIS), 2*(3), 249–268.

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change, 17*(2), 164-196.

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in fintech applications. *Sensors, 21*(5), 1594.

Tsapa, J. A. (2024). Predictive analytics for proactive risk management in fintech lending and investment. *Journal of Artificial Intelligence & Cloud Computing, 3*(1), 1–4.

Valli, L. N. (2024). Predictive analytics applications for risk mitigation across industries; a review. *BULLET: Jurnal Multidisiplin Ilmu, 3*(4), 542-553.

Zhou, Y., Li, H., Xiao, Z., & Qiu, J. (2023). A user-centered explainable artificial intelligence approach for financial fraud detection. *Finance Research Letters, 58*, 104309.