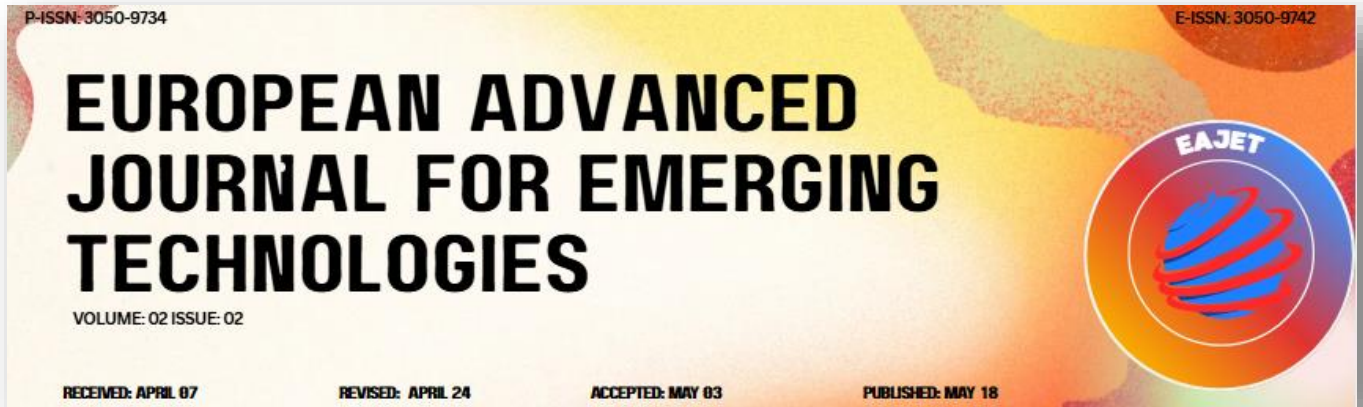




Governed Generative AI for Fraud and Wealth Risk

Olivia Johnson
Asst Professor

Abstract

Generative Financial Intelligence (GFI) is a formal framework that combines generative modelling with adaptive governance principles to address two core financial challenges: fraud detection and mitigation, and portfolio risk decisioning. By applying this dual focus, a GFI-enabled architecture supports trustworthy decision-making and satisfies the governance quality criteria established by the financial industry's fraud risk-management standards.

Underlying this framework is a general adaptive governance model designed for major data- and model-driven applications spanning fraud detection, fraud mitigation, and wealth management—one that informs a portfolio's long-term strategy. The model employs autonomous systems to anticipate likely outcomes, while explicitly acknowledging the uncertainty inherent in forecasting rare, high-impact events. Economic-inequality-driven systemic collapse, intensified by the 2020 pandemic, is one such event that leaves managed portfolios more vulnerable to external shocks. To address this, GFI validates model behaviour and feedback against closed-loop economic-data dynamics, generating rich scenario analyses for Adaptive Wealth and Portfolio Risk Management (AWPRM) and enabling real-time fraud mitigation.

GFI advances trustworthy AI in finance along two dimensions. First, it situates existing research on data-driven fraud detection and mitigation within a formal governance model for fraud management, enabling quality-assurance evaluation consistent with the organisational-design principles of the Fraud Risk Management Framework. Second, by leveraging generative models, GFI enables

principled uncertainty quantification and decision-making that strengthen portfolio risk governance.

Keywords—Generative Financial Intelligence; Fraud Hotspot Signal Processing; Generative Shape-Encoded Adversarial Networks; Generative Neural Coalition; A-TEAM; Real-Time Fraud Detection and Mitigation; Adaptive Portfolio Management; AI Governance for Finance; Wealth Risk Decisioning; Wealth Risk Management; Trustworthy Fraud Governance; Financial Risk Control; Geneva Finance; Global Governance; Risk Materialization Process; Dynamic Risk Governance; Generative Probabilistic Financial Models; Parametric Probabilistic Models; Generative Knowledge; Generative Models; Generative AI; Discriminative Models; Probabilistic Risk Models; Adaptive Wealth Risk Governance; Research-Policy Gap; Data Accessibility.

1. INTRODUCTION

A Generative Financial Intelligence Framework is articulated to support trustworthy fraud governance through real-time detection and mitigation of suspicious activity and by enabling adaptive decisioning for wealth risk management. Fraud governance is framed as a whole-of-society problem, centering on the design of institutions, electoral processes, agencies, and controls. Generative models are identified as the most suitable for operationalizing fraud governance because of their ability to combine probabilistic reasoning with the management of uncertainty, support automated compliance with regulatory requirements, and provide interpretable models. Governance quality

metrics provide a structured way of identifying the appropriate level of care for specific types of fraud. Governance quality considerations further inform the integration of safety, ethics, and audit dimensions into the development framework.

Generative Financial Intelligence denotes the design and operationalization of generative models to support intelligent decision-making in finance. The focus is on three specific aspects of finance: the detection and mitigation of fraudulent activity, the adaptive modelling of wealth risk, and compliance with regulatory requirements. Decision-making in these three areas typically exhibits a high level of uncertainty as a consequence of factors such as invisible adversaries, ever-changing market conditions, and model drift. The Generative Financial Intelligence framework comprises an architecture for the framework itself as well as the underlying data ingestion and provenance capabilities. The architecture consists of four modular layers: data, model, decision, and governance.

TABLE I. Four-Layer Architecture of the GFI Framework

Layer	Primary Function	Key Outputs / Artifacts
Data Layer	Ingestion, provenance tracking, lineage, quality-dimension monitoring	Cleansed datasets, schema/ontology metadata, audit trail
Model Layer	Hosts generative and discriminative models; uncertainty quantification	Trained models, posterior distributions, confidence intervals
Decision Layer	Converts model outputs into risk-based actions and thresholds	Fraud likelihood scores, hedging/decision triggers
Governance Layer	Applies quality indicators, safety, ethics, and audit criteria	Governance quality scorecards, sign-off records

TABLE II. Generative vs. Discriminative Models in Finance

Criterion	Discriminative Models	Generative Models
Quantity learned	Conditional distribution $P(Y X)$	Joint distribution $P(X, Y)$
Typical use	Class prediction for seen instances	Synthesizing plausible seen/unseen instances
Uncertainty handling	Point predictions with post-hoc UQ	Native probabilistic reasoning
Data efficiency	Needs more labeled samples	Better representations

Criterion	Discriminative Models	Generative Models
	in high-dimensional settings	with fewer samples
Role in GFI	Anomaly / fraud scoring	Posterior fraud likelihood, scenario generation

A. Fraud Governance as a Governance Problem

Fraud governance is a governance problem for which institutions are held accountable, and institutions are the group of stakeholders for whom fraud governance should be designed. Four questions must be answered to frame fraud governance as a governance problem:

- Which accounts for the institutional quality dimension of the governance quality triangle? The objective of a fraud governance system is to reduce fraud through the implementation of public policies designed according to the institutional design considerations examined to answer the previous question. Any reduction in the cost of fraud will benefit the institution and, consequently, all its stakeholders by reducing the fraudulent transfer of wealth from the private sector to the public purse and the subsequent ever-increasing tax burden on the law-abiding taxpayer.

- Who is responsible for fraud governance? The principal-agent relationship defines the responsibility of the institution to implement fraud governance.

Risk decisioning can be viewed as transferring wealth between those making the decision and the rest of the stakeholders, similar to a gamble or wager. However, when these stakeholders are not part of the decision-making process, the transfer from those not involved in the decision to those involved can lead to wealth creation for a very small group (i.e., hedge fund managers). When adopting a narrower definition, wealth risk decisioning can therefore be regarded as a governance problem involving a small subset of stakeholders, posing a slightly different question.

Mathematical Formulas:

$$(1) P(X, Y) = P(X | Y) P(Y) = P(Y | X) P(X)$$

Bayes' theorem decomposition of the joint distribution of inputs X and label Y (Section 2A).

$$(2) \text{ Discriminative model: } \theta = \arg \max_{\theta} \sum \log P_{\theta}(Y | X)$$

The discriminative strategy learns the conditional distribution directly from training data.

$$(3) \text{ Generative model: } \theta = \arg \max_{\theta} \sum \log P_{\theta}(X, Y)$$

The generative strategy learns the joint distribution, from which $P(Y|X)$ and $P(X)$ can both be derived.

$$(4) P(\text{Fraud} | x) = P(x | \text{Fraud}) P(\text{Fraud}) / P(x)$$

Posterior fraud likelihood produced by evaluating engineered transaction attributes x against the generative component.

(5) $\text{Action}(x) = \text{Mitigate if } S(x) \geq \tau, \text{ Escalate if } \tau_L < S(x) < \tau, \text{ Log if } S(x) \leq \tau_L$

Score-to-action mapping, where $S(x)$ is the fraud score and τ, τ_L are risk-based decision thresholds.

(6) $\text{VaR}\alpha(L) = \inf \{ l \in \mathbb{R} : P(L > l) \leq 1 - \alpha \}$

Standard value-at-risk formalization of the probabilistic, confidence-interval-based forecasts used in adaptive wealth risk decisioning at confidence level α .

2. Theoretical Foundations of Generative Financial Intelligence

Generative Financial Intelligence are defined within finance as probabilistic systems utilizing the methods of generative modelling; a family of machine learning systems capable of generating plausible instances of datasets along with label-configurable new seen/unseen data instances; clearly separated from the family of discriminative systems—predictors—capable of producing predictions for seen instances along with uncertainty quantification. The significance of generative financial systems becomes apparent through two considerations: Bayes Theorem and the Bayes-Bernoulli model. The former is the foundation of all probabilistic reasoning—natural as well as within the MLOps domain—and allows the coherent combination of independent probabilistic sources even across heterogeneous domains, while the latter quantifies uncertainty for a generic forecasting/modeling problem, crucial for confidence in decision-making and risk governance.

Generative Financial Intelligence is contextualized within theory of fraud governance; the formal confluence of signals, institutional design, regulatory control, typologies, and risk decisioning. Signals are a distinguished medium of information splicing between institutions and actors and the foundation of any creditability-based system; their internal integrity and external unity are essential pre-requirements for trust by stakeholders and by the general public. Formal constructs and corresponding design considerations are presented for the governance of signals in fraudulent situations and the application of these constructs to fraud detection and mitigation. A comprehensive review of the fraud governance literature—with emphasis on risk-based governance frameworks—and on the growing body of literature that discusses the governance aspects of Artificial Intelligence, Machine Learning, and Deep Learning, rounds off the contextualization.

Role in GFI	Anomaly / fraud scoring	Posterior fraud likelihood, scenario generation
-------------	-------------------------	---

TABLE III. Data Quality Dimensions Tracked in Provenance Management

Dimension	Governance Purpose
Accuracy	Ensures decisioning inputs reflect true underlying values
Completeness	Confirms no material gaps in transaction/portfolio records
Consistency	Aligns values across heterogeneous, multi-source data streams
Uniqueness	Prevents duplicate records from distorting risk/fraud scores
Timeliness	Supports real-time or near-real-time transaction evaluation
Validity	Confirms conformance to schema, ontology, and format rules
Relevance	Ensures ingested data materially informs decisioning goals

TABLE IV. Fraud Detection Technique Categories in the Delivery Framework

Technique Category	Description	Labeling Requirement
Statistical tests	Flags deviations from expected distributional behavior	None / minimal
Clustering	Groups transactions without prior labels to expose outliers	Unsupervised
Supervised anomaly classification	Learns to classify known fraud typologies	Labeled
Supervised anomaly detection	Learns boundary of normal behavior from labeled data	Labeled
Novelty discovery	Detects previously unseen fraud typologies	Semi-/unsupervised

A. Defining Generative Models in Finance

Generative models in finance are defined as supervised learning architectures that estimate the fundamental probability density function underlying a financial data domain by using labeled historical data for training, with labels indicating the appropriate data class category. They differ from discriminative models, which are supervised learning architectures that describe the conditional probability of the output, given the input specific to one or more class labels. Generative models afford various advantages over discriminative models: they enable probabilistic reasoning, capture latent variables, quantify

uncertainty, and offer better representations with less training data when the dimensions of the input space are large compared to the number of available training samples. Generative models may particularly benefit fraud detection and mitigation when accurately estimating the distribution of normal behavior and the underlying causal and contextual factors.

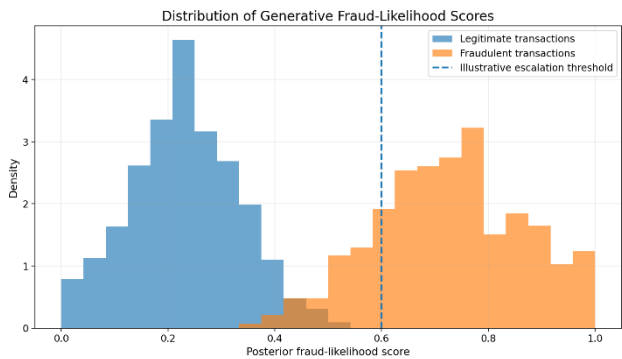
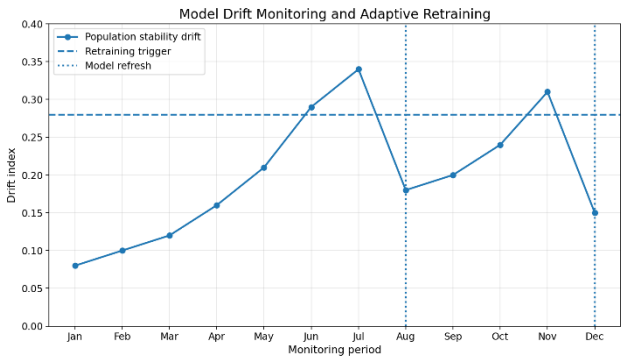
3. Architecture of the Framework

Piecewise modular construction fosters transparency, facilitates interlayer reuse, allows parallel development, and promotes safety; analytic components are naturally separated from datamap components, and unit-testing focus on specific algorithms remains possible even through a long data-processing pipeline. Notable aspects include the data lake and model layer, which contain all involved models and, by virtue of distinct input–target pairs, additionally the decisioning layer, which implements the decisioning procedures.

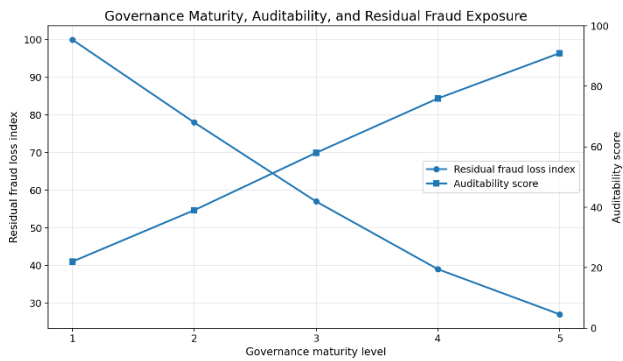
System design considers all data sources accessed in any manner. Data lineage and provenance support governance through transcriptability, reproducibility, and auditing. Data quality is monitored via coverage analysis and quality dimensions are documented. Provenance metadata, such as schema definitions and ontologies, facilitate queries from decision-makers and feed transformation functions. Privacy, confidentiality, and regulatory requirements inform access control, clustering, diffusion, and aggregation. Data availability, model drift, deviance from control emissions, and other aspects steered by proper data governance and quality management inform retraining and redocumentation cadences. Data-cleansing, feature-engineering, and transformation choices rest on domain knowledge.

Generative Financial Intelligence incorporates data ingestion, provenance tracking, and data quality management as prerequisites for reproducible decisioning. Source data include conventional structured and semi-structured datasets, unstructured non-relational sources such as news articles and social media streams, and content-rich relational business networks. Data acquisition employs a variety of methods appropriate to source type—scheduled file transfers or database exports, web scraping, application programming interfaces, and other programmed data retrieval techniques for non-relational sources. Provenance tracking incorporates lineage metadata addressing a wide range of data quality dimensions, including accuracy, completeness, consistency, uniqueness, timeliness, validity, and relevance; aligns the temporal characteristics of heterogeneous data streams; and manages privacy, confidentiality, and regulatory considerations. Data governance policies and access controls, review and audit trails, along with provenance metadata; ingestion actions integrating acquisition, cleansing, alignment, feature engineering, and transformation procedures; and schema and ontology design are captured in existing research. Provenance management and data governance are customarily enforced via dedicated underpinning layers.

Generative Financial Intelligence broadens participants’ decisioning toolkits, facilitating navigating uncertainty in candidate signal, risk, and decisioning models. Probabilistic forecasts of risk factors enable detection of changing relationships through analysis of model drift, while transparency supports sign-off of decision conditions. Governance quality determines updates and, in the case of major retraining, selection of redeployed models. Stress-testing scenarios thus include uncertainty quantification; drift-based reaction modelling; evolving hedging strategies; changes in liquidity and counterparty credit profile; monetary policy regimes; and the spatial, sectoral, and metamorphic attributes featured in related adaptable fraud detection and mitigation architectures.



A. Data Ingestion and Provenance



4. Adaptive Wealth Risk Decisioning Mechanisms

Modern wealth governance and risk decision processes operate in shrinking timeframes and with increasing transaction volumes. Consequently, instilling trust and confidence in key stakeholders is paramount. Trust and confidence require good governance, which in turn demands a clear understanding of the control environment; the factors that may impact the institution's activities; and the system's overall risk profile for the decision maker—in as close to real time as possible.

Adaptive Wealth Risk Decisioning Mechanisms are defined as methods that ascertain and communicate risk status in sufficient detail to allow informed decisioning at the speed of business for a manageable portfolio of plausible stress-testing scenarios. Possible decision types in wealth governance include portfolio hedging under liquidity and credit constraints, real-time fraud detection and mitigation, and the board and risk committee approval of risk-taking authority under a breach of tolerance for a black-swan event. Real-time fraud-detection and- mitigation has been discussed in the previous section.

A. Real-Time Fraud Detection and Mitigation

Real-time fraud detection and mitigation encompass mechanisms for processing streams of financial transactions, detecting anomalies and abnormal patterns, generating fraud likelihood scores, and triggering fraud management actions. This adaptation level includes an ingestion velocity compatible with processing transactions at source, such that transactions can be promptly evaluated against risk-based decision thresholds.

Fraud detection is aided by discriminative models or techniques designed to score anomalies. The delivery framework facilitates implementation of one or more models in these categories, including statistical tests, clustering without a-priori labels, supervised anomaly classification, supervised anomaly detection, or novelty discovery. Once scored, the original or engineered transaction attributes may be bundled and evaluated against a generative component to produce a posterior distribution of fraud likelihood. Such a score may be directed into an automated fraud mitigation control, logged for supervision and decision intelligence, or trigger human escalation depending on the score value,

latency and business returns associated with false omissions relative to false alarms.

5. Conclusion

The Generative Financial Intelligence framework advances trustworthy fraud governance and adaptive wealth risk decisioning through a formalized architectural specification that systematically integrates quality governance indicators. Data provenance preserves verifiability, reproducibility, and compliance with legal and regulatory requirements. Safety concerns encompass security and robustness against inputs of malicious intent, while a dedicated logging mechanism detects anomalies in both data and decisioning.

Acknowledging that deviation from normal behaviour is not sufficient for supervisory signals, a comprehensive mechanism for real-time detection and mitigation of fraud is proposed. A list of all potential fraud activity and related detection models flags abnormal patterns and assigns a likelihood of fraud. Adaptive portfolio and wealth risk modelling considers the impact of hypothetical extreme scenarios generated through generative components of the framework, and evaluates the viability of active portfolio and wealth risk decisioning. Uncertain risks are managed through probabilistic forecasts augmented with confidence intervals.

REFERENCES

1. Ashtiani, M. N., & Raahemi, B. (2022). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access*, 10, 72504–72525.
2. 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.
3. Zhu, X., Ao, X., Qin, Z., & others. (2021). Intelligent financial fraud detection practices in post-pandemic era. *The Innovation*, 2(4), 100176.
4. Pranitha Potturi. (2023). Cloud-Driven Business Intelligence Modernization for Scalable Enterprise Data Integration and Decision Support. *International Journal of Intelligent Systems and Applications in Engineering*, 11(3s), 387 –. Retrieved from <https://www.ijisae.org/index.php/IJISAE/article/view/8505>
5. Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, 131, 441–452.
6. Korol, V., & others. (2021). Usage of machine learning methods for early detection of money laundering schemes. *Procedia Computer Science*, 190, 184–192.
7. Hadji Misheva, B., Jaggi, D., Posth, J.-A., Gramespacher, T., & Osterrieder, J. (2021). Audience-dependent explanations for AI-based risk management tools: A survey. *Frontiers in Artificial Intelligence*, 4, 794996.
8. Sasidhar Reddy Mondeddu. (2023). Natural Language Processing for Intelligent Automation of Financial Documents and Banking Operations. *International Journal of Intelligent Systems and Applications in Engineering*, 11(8s), 605–612. Retrieved from <https://www.ijisae.org/index.php/IJISAE/article/view/8527>
9. Giudici, P., & Raffinetti, E. (2022). Explainable AI methods in cyber risk management. *Quality and Reliability Engineering International*, 38(3), 1318–1326.

10. Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2021). Explainable machine learning in credit risk management. *Computational Economics*, 57, 203–216.
11. Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in Artificial Intelligence*, 5, 779799.
12. Zhou, J., Chen, C., Li, L., Zhang, Z., & Zheng, X. (2022). FinBrain 2.0: When finance meets trustworthy AI. *Frontiers of Information Technology & Electronic Engineering*, 23(12), 1747–1764.
13. Mattaparthi, R. (2023). Deep Learning-Driven Combustion Anomaly Detection in Diesel Powertrains: A Multi-Sensor Fusion Approach for Real-Time ECM Adaptation. *International Journal of Intelligent Systems and Applications in Engineering*, 11, 1084.
14. Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., Ur Rehman, A., & Shafiq, M. (2022). Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. *Sustainability*, 14(21), 13875.
15. Tuffveson Jensen, R. I., & Iosifidis, A. (2023). Qualifying and raising anti-money laundering alarms with deep learning. *Expert Systems with Applications*, 214, 119037.
16. Alexandre, C. R., & Balsa, J. (2023). Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, 217, 119500.
17. Kolla, S. K., & Reddy, V. A. R. (2023). Deep Learning Architectures For Multimodal Medical Data Integration. *South Eastern European Journal of Public Health*, 248-260.
18. 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.
19. Zhang, T., Zhu, W., Wu, Y., Wu, Z., Zhang, C., & Hu, X. (2023). An explainable financial risk early warning model based on the DS-XGBoost model. *Finance Research Letters*, 56, 104045.
20. Khan Achakzai, M. A., & Peng, J. (2023). Detecting financial statement fraud using dynamic ensemble machine learning. *International Review of Financial Analysis*, 89, 102827.
21. Aftabi, S. Z., Ahmadi, A., & Farzi, S. (2023). Fraud detection in financial statements using data mining and GAN models. *Expert Systems with Applications*, 227, 120144.
22. Loganathan, R. (2022). Converging Security Architecture and Compliance Management in Enterprise Data Center Ecosystems: A Unified Control Framework. *International Journal of Scientific Research and Modern Technology*, 1(12), 295-312.
23. Bhowmik, A., Sannigrahi, M., Chowdhury, D., & Dwivedi, A. D. (2022). DBNex: Deep belief network and explainable AI based financial fraud detection. In 2022 IEEE International Conference on Big Data (Big Data). IEEE.
24. Alonso Robisco, A., & Carbó Martínez, J. M. (2022). Measuring the model risk-adjusted performance of machine learning algorithms in credit default prediction. *Financial Innovation*, 8, 70.
25. Cummins, M., Gogolin, F., Kearney, F., & Kiely, G. (2022). Practice-relevant model validation: Distributional parameter risk analysis in financial model risk management. *Annals of Operations Research*, 318, 107–131.
26. Gouriéroux, C., & Monfort, A. (2021). Model risk management: Valuation and governance of pseudo-models. *Econometrics and Statistics*, 17, 1–22.
27. Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, 62, 101744.
28. Bharath Penaka. (2023). AI-Driven Predictive Analytics for Early Detection of High-Risk Patients in Cloud-Based Healthcare Systems . *International Journal of Medical Toxicology and Legal Medicine*, 26(3 and 4), 118–124. Retrieved from <https://ijmtlm.org/index.php/journal/article/view/1506>
29. Shabsigh, G., & Boukherouaa, E. B. (2023). Generative artificial intelligence in finance: Risk considerations. IMF FinTech Note 2023/006. International Monetary Fund.
30. Chen, H. (2023). Large language models in finance: A survey. In *Proceedings of the Fourth ACM International Conference on AI in Finance* (pp. 374–382). Association for Computing Machinery.
31. Eddin, A. N., Bono, J., Aparício, D., Polido, D., Ascensão, J. T., Bizarro, P., & Ribeiro, P. (2021). Anti-money laundering alert optimization using machine learning with graphs. arXiv.