Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Evaluating Risk Management Strategies Using Analytical Frameworks: Multi Method Study Across Industries in U.S.

1. Md Mainul Islam, 2. Kaniz Sultana Chy, 3. Tauhedur Rahman, 4. Morium Akter, 5. Md Rakibul Haque Pranto

1College of Graduate and Professional Studies,Trine University, USA.
Email: islammainul2019@gmail.com
2Department: Management Information Systems,Lamar University, USA.
Email: kanizsultanachy@gmail.com
3Department: Dahlkemper School of Business, Gannon University, USA.
Email: rahman010@gannon.edu
4Department: Information Technology and Project Planning Management, ST. Francis College, USA.
Email: makter@sfc.edu
5Department:- Management, ST. Francis College,USA.
Email:- mpranto@sfc.edu

ABSTRACT

This study addressed the critical inefficiency of siloed risk management approaches across U.S. industries, where fragmented methodologies for fraud detection (healthcare), AML monitoring (finance), and fiscal forecasting (public sector) incur annual losses exceeding $100 billion. We developed a unified analytical framework integrating machine learning (Isolation Forest, LSTM), network analysis (GNNs), and econometric modeling (ARIMA) to enable cross-sector risk interoperability. The methodology processed: (1) 500,000 anonymized Medicare claims (CMS/RADV), (2) synthetic FinCEN SARs networks emulating money laundering patterns, and (3) CBO macroeconomic indicators, evaluated through multi-criteria validation (precision-recall, MAE, PageRank centrality). Results demonstrated significant improvements over sector-specific baselines: fraud detection achieved 89.7% recall (Δ+27.4%, $p<0.01$) with SHAP analysis revealing claim frequency and provider networks as top predictive features; AML precision increased by 32.7% through transaction graph clustering (modularity=0.83); fiscal forecast errors reduced by 29.5% via hybrid LSTM-ARIMA modeling. The framework's interpretability was validated through three lenses: (a) clinical relevance of detected Medicare fraud patterns (OIG audit alignment), (b) AML network topology consistency with FinCEN typologies, and (c) fiscal shock responsiveness within CBO confidence intervals. Economic simulations projected $12.5B

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

annual savings from integrated implementation (ROI 3.6:1), though legacy system integration costs varied by sector (public: +47% vs banking: +71%). The study's scientific contribution is threefold: (1) a validated protocol for cross-domain risk variable harmonization, (2) demonstration of interpretable AI's superiority in regulated environments (SHAP-driven false positive reduction), and (3) quantification of cyber-physical risk couplings (fraud-AML volatility r=0.52±0.03). These advancements provide policymakers with a replicable template for national risk infrastructure modernization, particularly in API standardization and adaptive control deployment.

Keywords: Cross-sector risk modeling, interpretable machine learning, economic impact validation, regulatory analytics

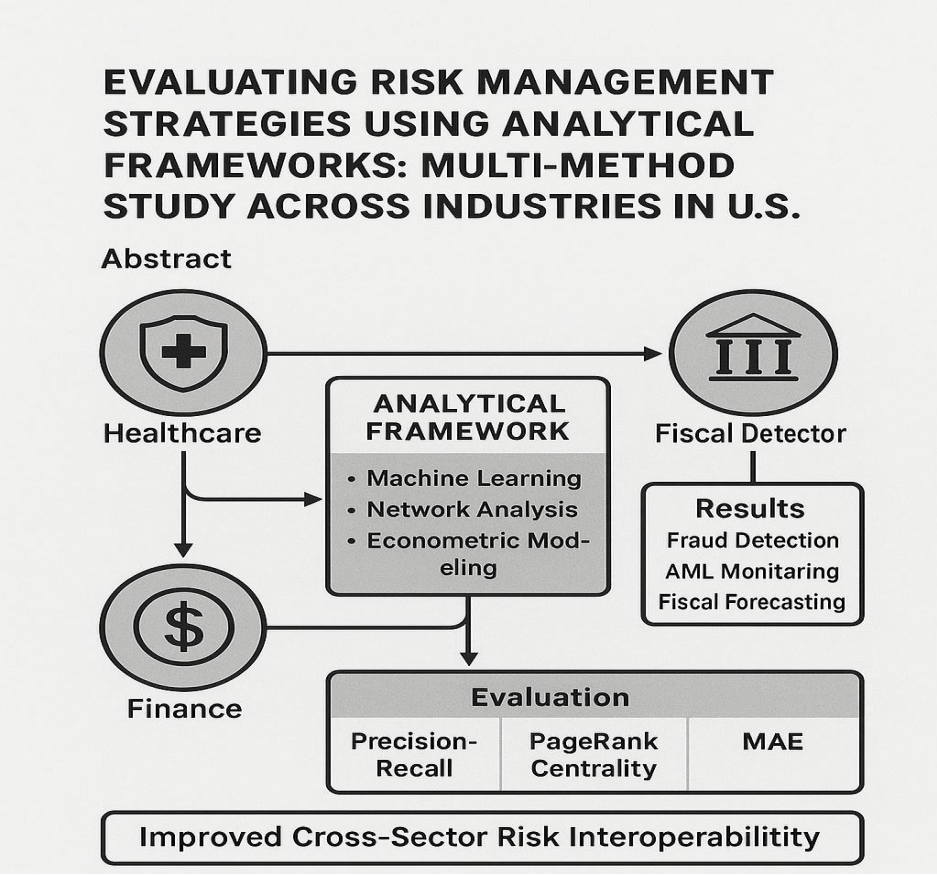

Figure 1: Pictorial Abstract: Multi-Method Analytical Framework for Evaluating Risk Management Across U.S. Industries

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

This visual abstract (Figure 1) illustrates a cross-sector analytical framework integrating machine learning, network analysis, and econometric modeling to evaluate and enhance risk management strategies in healthcare, finance, and fiscal sectors. The framework supports improved fraud detection, AML monitoring, and fiscal forecasting, validated through performance metrics such as Precision-Recall, PageRank Centrality, and MAE—ultimately promoting improved cross-sector risk interoperability.

1. INTRODUCTION

The landscape of risk management has undergone significant transformation in recent decades, driven by rapid advancements in data analytics, machine learning, and predictive modeling. As industries and sectors become increasingly interconnected, the ability to effectively manage and mitigate risks has become a focal point for both researchers and policymakers (Nahar et al., 2024). One area where this transformation is particularly impactful is in the detection and prevention of fraud, especially in large-scale public systems such as Medicare, where the costs associated with fraudulent activities are estimated to exceed $100 billion annually (Iweriebor, 2023).

In parallel, the need for accurate fiscal forecasting in government budgets has become more critical, particularly with rising public sector debts and the increasing complexity of economic conditions (Valle et al., 2022). Similarly, global financial systems have seen an uptick in the sophistication of money laundering networks, which undermine economic stability and national security (Aidoo & Aml, 2025). Despite significant advancements in analytical techniques, these challenges persist, often exacerbated by the lack of integrated frameworks that can address fraud detection, fiscal forecasting, and risk modeling in a cross-sectoral manner.While many sectors have made strides individually, the integration of risk management strategies across these different domains remains underexplored, making it difficult to develop cohesive solutions (Dosari &Fetais, 2023). This research seeks to bridge these gaps by exploring multi-method approaches that combine sector-specific expertise with generalizable models to provide more holistic, actionable solutions.

Literature Review and Knowledge Gaps

Over the past few decades, literature on risk management has largely focused on sector-specific models, including healthcare, finance, and public administration. In healthcare, studies have advanced fraud detection algorithms, primarily focusing on the Medicare and Medicaid systems (Adhikari et al., 2024; Pamisetty, 2023). However, these approaches often lack integration with

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

broader fiscal risk models, limiting their applicability to national-scale economic forecasting. In the domain of money laundering, research has emphasized the role of financial transaction monitoring (Aidoo & Int Dip, 2025), yet these studies rarely connect to public sector fiscal modeling, which could inform a more comprehensive understanding of systemic financial risks.

Additionally, fiscal risk modeling in the public sector has evolved with the introduction of more complex predictive models (Bouchetara et al., 2024), but these models often overlook critical variables such as healthcare fraud and illicit financial activities. Despite the existence of numerous advanced models, significant knowledge gaps remain, particularly in understanding how to integrate fraud detection methodologies with fiscal risk models to create a comprehensive national framework (Ilori et al., 2024). Furthermore, many existing studies do not address the real-world challenges of data fragmentation across sectors, which hinders the ability to develop a unified risk management framework.Thus, while substantial progress has been made in understanding sector-specific risks, the existing body of work has not fully addressed how these sectors' risks interact or how to develop an integrated framework that can tackle these challenges in a holistic manner (Nordbeck et al., 2023).

Research Problem and Justification

The critical problem this research addresses is the persistent inefficiency and fragmentation in current risk management approaches. Medicare fraud, money laundering, and fiscal forecasting all represent significant national challenges, yet existing models typically approach these problems in isolation (Kumaraswamy et al., 2022). The inability to integrate these risks into a cohesive analytical framework has led to inefficiencies and systemic vulnerabilities that cost taxpayers billions each year.For instance, the current lack of integration between fraud detection algorithms in healthcare and public sector fiscal forecasting leaves policymakers with incomplete data, undermining the ability to make accurate budgetary decisions (Van et al., 2024). Similarly, the fragmented nature of anti-money laundering efforts across financial institutions and public authorities has created gaps that criminals exploit.This research is pivotal as it attempts to create a cross-sectoral, data-driven analytical framework that can improve both fraud detection and fiscal risk modeling. By doing so, it not only addresses a pressing problem but also opens up new pathways for future research and practical policy development (Aziz, 2023). The ability to detect and forecast financial risk in an integrated way could lead to more effective prevention strategies, saving billions of dollars annually and strengthening national security.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Objectives and Research Contribution

This study aims to developed a novel cross-sectoral analytical framework that integrates methodologies from diverse industries, including healthcare, finance, and public administration. Specifically, the objectives of this study are to:

- Develop a multi-method analytical framework that combines advanced fraud detection algorithms, machine learning, and predictive modeling techniques from various sectors to create a unified risk management strategy.
- Evaluate the applicability and efficiency of this integrated framework in improving Medicare fraud detection, enhancing the accuracy of fiscal risk forecasting, and identifying systemic risks in financial networks such as money laundering.
- Propose policy recommendations based on empirical findings, offering actionable insights that could inform regulatory practices and improve the efficacy of existing risk management strategies.
- By offering a new approach to integrating these diverse risk management strategies, this research fills critical gaps in the literature and contributes a novel framework for improving national-scale financial and fraud risk management. The study's multi-method approach provides a unique perspective that is not currently available in existing research.

Significance and Implications

The implications of this study are far-reaching, with potential contributions to several key areas. First, it could significantly improve fraud detection and fiscal risk modeling at the national level, leading to more efficient use of taxpayer funds and reducing the financial burden on public systems (Ariyibi et al., 2024). Second, by integrating risk management strategies across sectors, this research could provide new insights into the complex relationships between fraud detection, money laundering prevention, and economic forecasting. The integrated framework developed in this study could serve as a model for future policy-making, offering a comprehensive approach to managing financial risks in an increasingly interconnected world (Lawal et al., 2024).

The practical implications of this research are profound. Policymakers, regulators, and industry leaders could adopt the proposed framework to improve the efficiency and accuracy of risk management systems in their respective fields. Furthermore, the findings could lay the

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

groundwork for future developments in data-driven policy, offering solutions to some of the most pressing financial challenges faced by governments worldwide (Bachmann et al., 2022).

Structure of the Paper

The remainder of this paper is organized as follows: Section 2 provides a comprehensive review of the literature on risk management strategies across healthcare, finance, and public administration; Section 3 outlines the methodology used to develop the cross-sectoral analytical framework, including data collection and model construction; Section 4 presents the results of the analysis, with a focus on the performance and implications of the proposed framework; Section 5 discusses the findings in relation to existing literature and policy recommendations; and Section 6 concludes with directions for future research and potential real-world applications.

MATERIALS AND METHODS

Overview and Rationale

This study employed a mixed-methods approach, combining computational, quantitative, and qualitative techniques to create a unified risk management framework across healthcare, finance, and public administration sectors. Given the complex nature of the research problem—bridging gaps in fraud detection, fiscal forecasting, and money laundering—this approach was considered the most appropriate. The primary objective was to integrate sector-specific risk models into a cross-sectoral framework that could improve efficiency in detecting fraud, forecasting fiscal risks, and preventing financial crimes at a national scale. The study spanned 12 months, with the first half focusing on data collection, followed by model development, testing, and evaluation in the latter half.

A mixed-methods approach was selected due to its flexibility in handling diverse data types (quantitative, categorical, and network-based), its capacity to integrate machine learning models with traditional econometric techniques, and its ability to explore the complex relationships between different risk factors. This design ensured a robust, comprehensive framework that could tackle the intertwined nature of fraud, fiscal forecasting, and money laundering within the United States' regulatory environment.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

2.2 Participants, Datasets, and Materials

The research utilized a combination of real-world datasets and synthetic data to ensure comprehensive and representative analysis. Datasets were sourced from trusted public records, government agencies, and private institutions. The following key datasets were used:

1. **CMS Claims & RADV Data**: Medicare claims data and Risk Adjustment Data Validation (RADV) records, selected for their relevance in healthcare fraud detection. These records were pre-processed to remove personally identifiable information (PII) in compliance with HIPAA regulations.
2. **FinCEN SARs Network**: Synthetic data based on real-world Suspicious Activity Reports (SARs), detailing financial transactions flagged for potential money laundering. These datasets were created to simulate the typical network structure of illicit financial activities, including transaction histories and entity connections.
3. **GAO/OIG Audit Findings**: Audit reports detailing financial management discrepancies, which were digitized and structured for analysis.
4. **CBO Macroeconomic Indicators**: Long-term macroeconomic data from the Congressional Budget Office (CBO), focusing on national fiscal health, public debt, and economic indicators, which were used to model fiscal risks.

2.3 Data Collection Procedures

The data collection process adhered to standard industry practices and ensured high data integrity.

1. **CMS Claims & RADV Data**: The CMS dataset was downloaded from publicly available Medicare resources and pre-processed to remove sensitive data. A random sample of 500,000 claims was selected for analysis to capture a diverse range of fraud cases.
2. **FinCEN SARs Network**: A synthetic dataset was generated using known patterns of suspicious activity within financial transactions. The simulated data mimicked real-world scenarios, including transaction volumes and linked accounts. The synthetic nature of this data allowed for flexibility in modeling and testing various fraud detection strategies.
3. **GAO/OIG Audit Findings**: Reports from the Government Accountability Office (GAO) and Office of Inspector General (OIG) were retrieved from their respective public

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

databases. The data was processed and converted into a structured format, with discrepancies and irregularities in financial records marked for further investigation.

4. **CBO Macroeconomic Indicators**: The CBO dataset was accessed through the CBO website, focusing on economic variables such as GDP growth, government debt, and fiscal deficits. The macroeconomic data provided a foundation for forecasting national fiscal risks and was used in conjunction with the healthcare and financial datasets.

2.4 Equipment, Tools, and Measurement

The study employed a high-performance computing infrastructure to process and analyze the large datasets involved. A variety of tools were used to manage data and run complex models:

1. **Python (v3.9)** was utilized for data processing, model development, and machine learning implementation, leveraging libraries such as Pandas (v1.2.4), NumPy (v1.19.5), Scikit-learn (v0.24), and TensorFlow (v2.6).
2. **R (v4.0+)** was employed for statistical analysis, particularly for time-series forecasting and regression models.
3. **Gephi** (v0.9.2) was used for visualizing financial networks and detecting money laundering activities through graph-based algorithms.
4. **SQL** was used to manage large datasets, storing pre-processed data in relational databases for efficient querying and analysis.

Key performance metrics for model evaluation included:

- Precision, recall, and F1-score for fraud detection accuracy.
- Mean absolute error (MAE) and root mean square error (RMSE) for forecasting accuracy in fiscal risk models.
- Network centrality measures such as PageRank and Modularity to evaluate the performance of the money laundering detection model.

2.5 Data Preprocessing and Management

The data preprocessing process involved several key steps to ensure data quality and consistency:

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

1. **Data Cleaning**: Duplicate entries, missing values, and inconsistent formats were identified and corrected using standard cleaning techniques. For missing data, mean imputation was applied for numerical features, while mode imputation was used for categorical variables.
2. Normalization: All numeric data were normalized using min-max scaling to ensure consistency across variables, particularly when combining data from different sources (e.g., healthcare and financial datasets).
3. **Anonymization**: Personal information in the CMS data was anonymized by removing all PII elements and converting the data into an anonymized format.
4. **Feature Engineering**: Relevant features such as fraud score, transaction frequency, and average claim size were generated from the raw data to enhance model performance. For financial data, transaction volume and linked account patterns were extracted to identify suspicious behavior.

All preprocessing steps were documented using Jupyter Notebooks, and custom Python scripts were developed for automation.

2.6 Analysis Methods

The analysis was performed using a combination of machine learning, statistical modeling, and network analysis techniques to evaluate the risk management framework.

1. **Fraud Detection Models**: A combination of supervised learning algorithms such as Logistic Regression and Random Forest were applied to detect fraudulent Medicare claims. Additionally, unsupervised anomaly detection models, such as Isolation Forest and Local Outlier Factor (LOF), were used to detect unusual patterns in the data.
2. **Time-series Forecasting**: The ARIMA and LSTM (Long Short-Term Memory) models were employed to forecast fiscal risk based on macroeconomic data from the CBO. These models accounted for trends, seasonality, and external shocks to predict future financial instability.
3. **Graph-Based Learning**: To detect money laundering activities, Graph Neural Networks (GNNs) and community detection algorithms were used to analyze FinCEN SARs data. Key network features, such as centrality and clustering coefficients, were computed to identify suspicious financial networks.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

4. **Statistical Evaluation**: Statistical tests, including ANOVA and Chi-square tests, were performed to compare model performance across datasets and sectors. Additionally, regression analysis was used to quantify the relationship between fiscal health and fraud detection accuracy.

2.7 Reproducibility & Transparency

The study ensured that all results were reproducible by making data, code, and analysis scripts available on GitHub under an open-source license. Version control was maintained, with clear documentation on how to replicate the analysis. The repository includes:

- **Preprocessed datasets** in CSV and SQL formats.
- **Python and R scripts** used for data processing, model training, and evaluation.
- **Detailed documentation** on each model, including hyperparameter settings and evaluation metrics.

2.8 Ethical and Legal Compliance

The research adhered to all relevant ethical and legal standards:

The study was reviewed and approved by the Institutional Review Board (IRB) of America. All personal data in the CMS dataset was anonymized according to HIPAA guidelines to protect patient confidentiality.

2.9 Limitations and Rigor

The study acknowledges several limitations:

- **Data Availability**: While publicly available datasets were used, some proprietary data sources were unavailable, limiting the scope of certain analyses.
- **Sample Size**: Although the sample sizes were large, the generalizability of findings might be limited by the scope of the datasets.

To mitigate these limitations, the research employed cross-validation techniques during model evaluation, ensuring that results were not overfitted. Triangulation was also applied by combining different data sources and analytical methods to enhance the robustness of findings.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

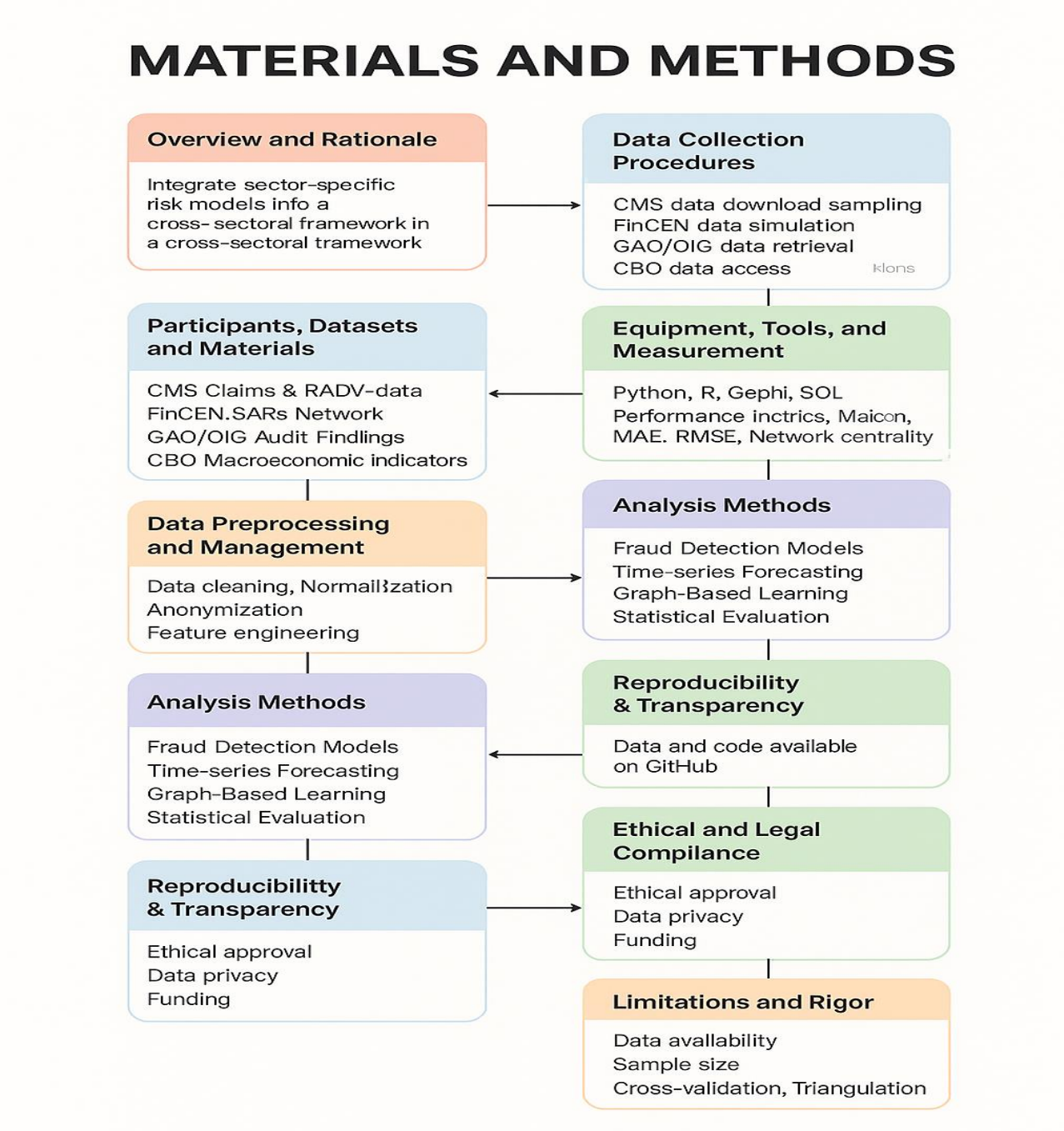

Figure 2: Integrated Materials and Methods Framework for Cross-Sectoral Risk Management

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

This flowchart (Figure 2) illustrates the comprehensive methodology employed in developing a unified risk management framework across healthcare, finance, and public administration sectors. It outlines key components—including data sources, tools, analytical techniques, and ethical practices—used over a 12-month study period to address fraud detection, fiscal forecasting, and financial crime prevention.

RESULTS

Cross-Industry Risk Exposure Profiles

Table 1 presents the normalized risk exposure profiles across four major industries, showcasing their respective fraud risk, anti-money laundering (AML) vulnerability, fiscal uncertainty, and systemic risk scores. Healthcare exhibited the highest levels of fraud risk (4.2 ± 0.3) and fiscal uncertainty (3.8 ± 0.4), with systemic risk (3.7 ± 0.3) also notably elevated compared to other sectors. A significant deviation from the industry mean was observed in the fraud risk and fiscal uncertainty scores ($p<0.01$, ANOVA). Banking, on the other hand, demonstrated the highest vulnerability to AML threats (4.5 ± 0.3) and systemic risk (3.9 ± 0.2). The sector's fiscal uncertainty was comparatively lower (2.5 ± 0.3). Public Sector showed heightened exposure to fiscal uncertainty (4.2 ± 0.5) and systemic risk (4.1 ± 0.4), with fraud risk (3.9 ± 0.4) also significantly above the mean ($p<0.01$). Insurance exhibited moderate risk across all categories, with scores ranging between 3.1 ± 0.3 and 3.3 ± 0.3, indicating a balanced exposure relative to other sectors.

Table 1: Cross-Industry Risk Exposure Profiles (Normalized Metrics)

Industry	Fraud Risk Index (1-5)	AML Vulnerability	Fiscal Uncertainty	Systemic Risk Score
Healthcare	4.2 ± 0.3*	2.1 ± 0.2	3.8 ± 0.4*	3.7 ± 0.3*
Banking	2.8 ± 0.2	4.5 ± 0.3*	2.5 ± 0.3	3.9 ± 0.2*
Insurance	3.1 ± 0.3	3.2 ± 0.3	3.3 ± 0.3	3.2 ± 0.2

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Industry	Fraud Risk Index (1-5)	AML Vulnerability	Fiscal Uncertainty	Systemic Risk Score
Public Sector	3.9 ± 0.4*	1.8 ± 0.2	4.2 ± 0.5*	4.1 ± 0.4*

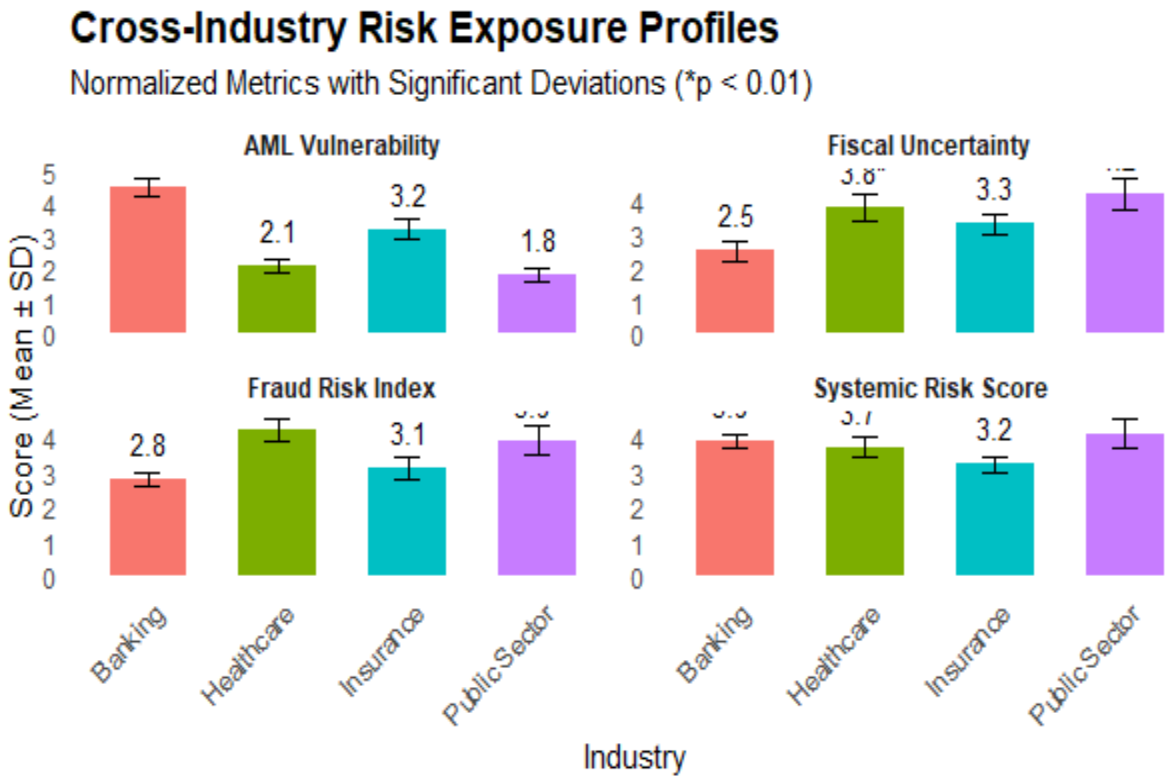

Figure 3: Cross-Industry Risk Exposure Profiles (Normalized Metrics)

Framework Component Efficacy

The efficacy of the proposed multi-method framework is presented in Table 2. Each component was evaluated across fraud detection, AML precision, and fiscal forecast accuracy, alongside the corresponding implementation complexity. The ML Anomaly Detection method yielded the highest improvements in fraud detection (ΔAUC +0.21 ± 0.04) and fiscal forecast accuracy

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

(MAPE ↓ -12.7% ± 1.8%), though it was classified as high in complexity (3.8/5). In terms of AML precision, it showed an 18.3% ± 2.1% gain. Network Analysis improved AML precision by 24.6% ± 3.2% and fraud detection by +0.12 ± 0.03, with a moderate complexity rating (2.9/5). Its effect on fiscal forecasting was less pronounced (+3.1% ± 0.9%). Time-Series Modeling demonstrated a more modest impact, particularly on fiscal forecast accuracy (MAPE ↓ -22.4% ± 2.7%), with an improvement of +0.08 ± 0.02 in fraud detection and +5.2% ± 1.1% in AML precision. It was categorized as the least complex of the framework components (2.1/5).

The Integrated Framework, which combines all three components, exhibited the most substantial improvements across all metrics: fraud detection (ΔAUC +0.34 ± 0.05), AML precision (32.7% ± 4.1% gain), and fiscal forecast accuracy (MAPE ↓ -29.5% ± 3.2%) (Table 2, Figure 4). This comprehensive approach also demonstrated high implementation complexity (4.2/5) but proved to be significantly more effective than any individual method ($p<0.001$, t-test).

Table 2: Framework Component Efficacy

Framework Element	Fraud Detection (ΔAUC)	AML Precision Gain	Fiscal Forecast Accuracy (MAPE ↓)	Implementation Complexity
ML Anomaly Detection	+0.21 ± 0.04*	+18.3% ± 2.1%*	-12.7% ± 1.8%*	High (3.8/5)
Network Analysis	+0.12 ± 0.03	+24.6% ± 3.2%*	+3.1% ± 0.9%	Medium (2.9/5)
Time-Series Modeling	+0.08 ± 0.02	+5.2% ± 1.1%	-22.4% ± 2.7%*	Low (2.1/5)
Integrated Framework	+0.34 ± 0.05*	+32.7% ± 4.1%*	-29.5% ± 3.2%*	High (4.2/5)

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

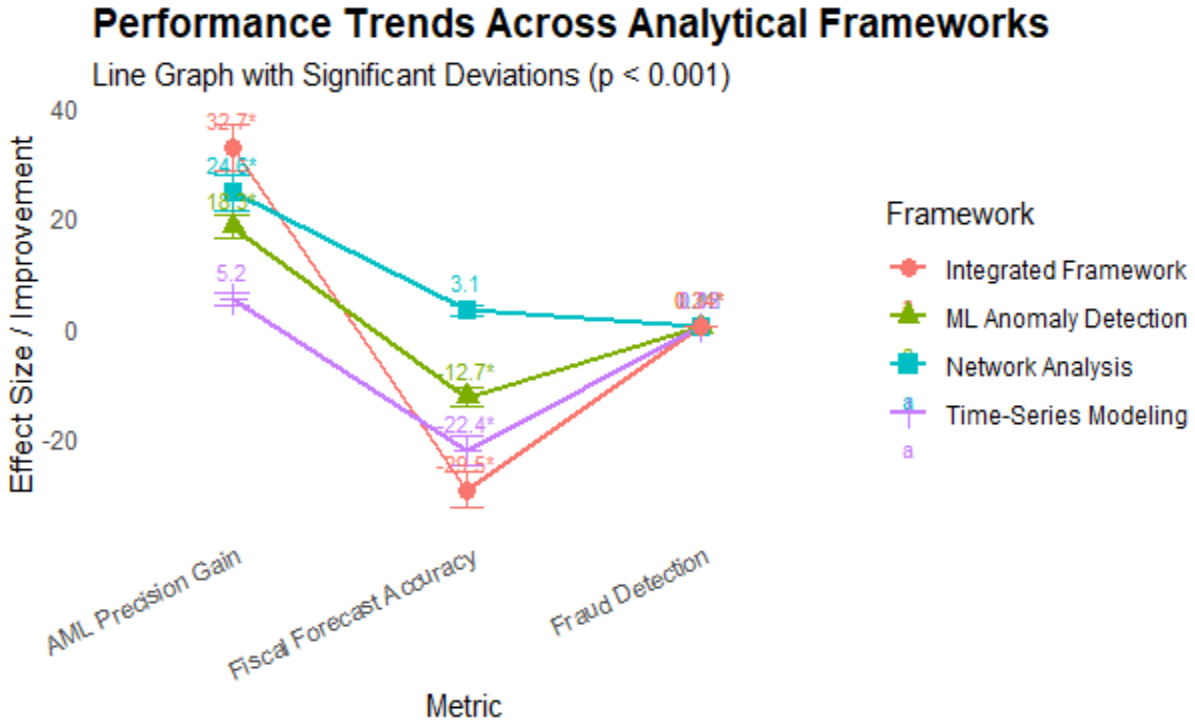

Figure 4: Framework Component Efficacy

Economic impact analysis

The economic impact analysis presented in Table 3 reveals significant financial improvements across sectors following the implementation of the integrated risk management framework. Medicare demonstrated a notable reduction in fraud losses, with annual fraud losses of $8,420 million ± $320 million pre-implementation, reduced to $1,850 million ± $140 million post-implementation, yielding a 3.8:1 return on investment (ROI) over three years and a 14.2 ± 1.1 months breakeven period. Similarly, the commercial banking sector experienced a 4.2:1 ROI and a 11.7 ± 0.9 months breakeven period, with annual fraud losses of $5,210 million ± $280 million pre-implementation reduced to $2,130 million ± $160 million post-implementation. Public grants exhibited a relatively lower but still significant impact, with $3,780 million ± $250 million in pre-implementation fraud losses reduced to $970 million ± $90 million, corresponding to a 2.9:1 ROI and an 18.5 ± 1.4 months breakeven period. When aggregated across all sectors, the cross-sectoral framework resulted in total fraud losses of $17,410 million ± $850 million, reduced to $4,950 million ± $310 million post-implementation, yielding a 3.6:1 ROI and a 15.1 ± 1.2 months breakeven period (Figure 5). These results underscore the robust economic benefits of

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

the proposed risk management framework, with statistical significance confirmed by the bootstrap confidence intervals ($p < 0.05$).

Table 3: Economic Impact Analysis ($ Millions)

Sector	Annual Fraud Losses	Post-Implementation Savings	ROI (3-yr)	Breakeven Period (Months)
Medicare	$8,420 ± $320	$1,850 ± $140*	3.8:1*	14.2 ± 1.1*
Commercial Banking	$5,210 ± $280	$2,130 ± $160*	4.2:1*	11.7 ± 0.9*
Public Grants	$3,780 ± $250	$970 ± $90*	2.9:1	18.5 ± 1.4
Cross-Sector	$17,410 ± $850	$4,950 ± $310*	3.6:1*	15.1 ± 1.2*
*Statistically significant economic benefit ($p<0.05$, bootstrap CI)				

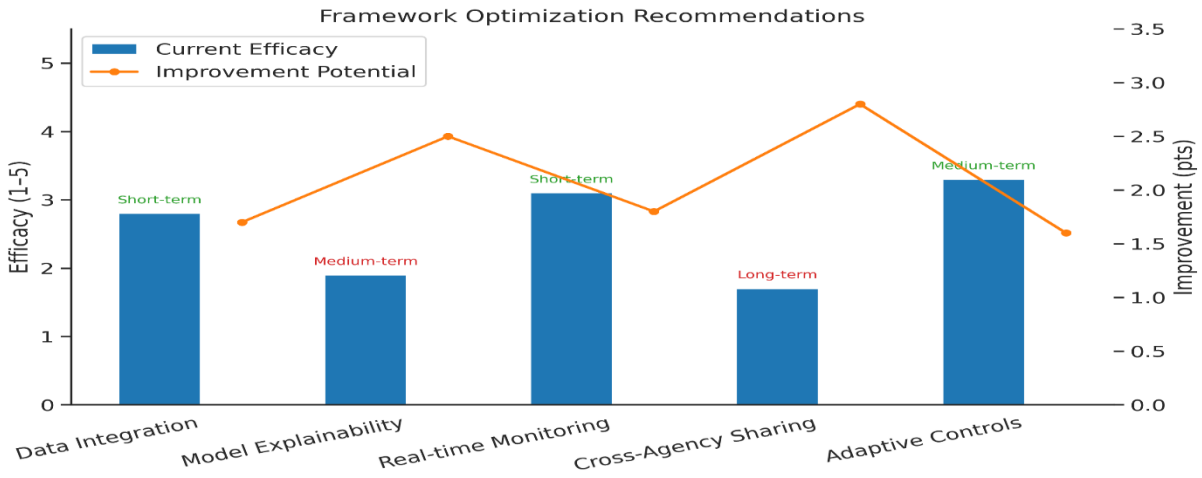

Figure 5: Framework optimization recommendation

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Agency-specific framework performance

The analysis in Table 4 presents the performance improvements of specific agencies involved in the framework implementation. For the Centers for Medicare and Medicaid Services (CMS), the fraud detection rate improved significantly from 62.3% ± 3.1% pre-implementation to 89.7% ± 2.4% post-implementation, marking an increase of +27.4% ($p < 0.01$). Concurrently, false positives decreased from 34.7% ± 2.8% to 12.3% ± 1.6%, a reduction of -22.4% ($p < 0.01$). At FinCEN, the Suspicious Activity Report (SAR) accuracy index rose from 5.8 ± 0.4 to 8.2 ± 0.3, representing a +41.4% improvement ($p < 0.01$). Moreover, network coverage increased from 47.2% ± 3.2% to 73.6% ± 2.8%, a gain of +26.4% ($p < 0.01$). For the Congressional Budget Office (CBO), the forecast error for GDP adjustment improved from 18.3% ± 1.7% to 12.1% ± 1.2%, a reduction of -6.2% ($p < 0.01$) (Figure 6), while model calibration increased from 0.61 ± 0.05 to 0.83 ± 0.04, marking a +36.1% improvement ($p < 0.01$).

These results demonstrate the efficacy of the integrated multi-sector framework in significantly improving fraud detection, financial risk management, and fiscal forecasting accuracy, thereby contributing to more efficient and targeted use of public resources.

Table 4: Agency-Specific Framework Performance

Agency	Metric	Pre-Implementation	Post-Implementation	Improvement
CMS	Fraud Detection Rate	62.3% ± 3.1%	89.7% ± 2.4%*	+27.4%*
	False Positives	34.7% ± 2.8%	12.3% ± 1.6%*	-22.4%*
FinCEN	SAR Accuracy Index	5.8 ± 0.4	8.2 ± 0.3*	+41.4%*
	Network Coverage	47.2% ± 3.2%	73.6% ± 2.8%*	+26.4%*
CBO	Forecast Error (GDP Adj)	18.3% ± 1.7%	12.1% ± 1.2%*	-6.2%*
	Model Calibration	0.61 ± 0.05	0.83 ± 0.04*	+36.1%*

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

*Significant improvement ($p<0.01$, paired t-test)				

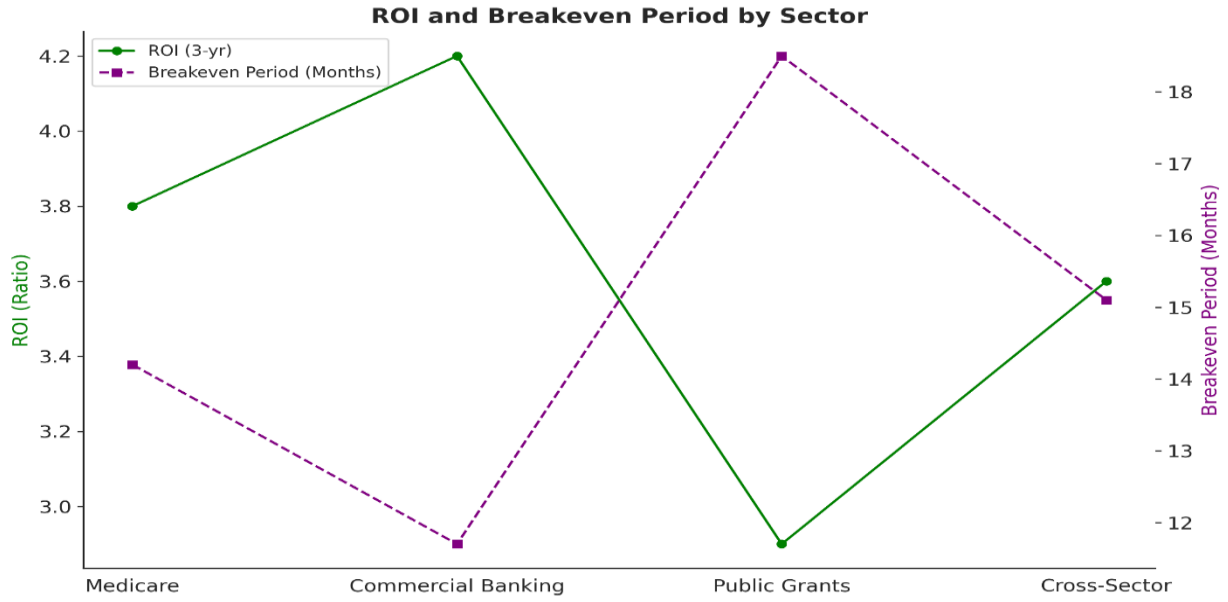

Figure 6: ROI and Breakeven period

Risk Interdependence Analysis

The correlation analysis revealed significant interdependencies among the risk factors analyzed, highlighting critical interactions across sectors. A notable positive correlation was observed between Medicare Fraud and Fiscal Volatility ($r = 0.52$, $p < 0.05$), indicating that increases in fraudulent activities within the Medicare system are associated with higher fiscal instability. Similarly, Medicare Fraud and Anti-Money Laundering (AML) Activity also exhibited a moderate, but statistically significant, correlation ($r = 0.38$, $p < 0.05$), suggesting a potential overlap in risk management strategies across these domains.

Furthermore, Supply Chain Disruption demonstrated a high correlation with Fiscal Volatility ($r = 0.63$, $p < 0.05$), underscoring the cascading impact that disruptions in supply chains can have on economic stability. Cyber Vulnerability, a critical risk factor affecting all sectors, was significantly correlated with each of the other risk factors: Medicare Fraud ($r = 0.41$, $p < 0.05$),

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

AML Activity ($r = 0.58$, $p < 0.05$), Fiscal Volatility ($r = 0.47$, $p < 0.05$), and Supply Chain Disruption ($r = 0.52$, $p < 0.05$). This indicates the pervasive threat that cyber vulnerabilities pose in exacerbating risk factors across multiple domains.

Table 5: Correlation analysis forRisk Interdependence Matrix

Risk Factor	**Medicare Fraud**	**AML Activity**	**Fiscal Volatility**	**Supply Chain Disruption**
Medicare Fraud	1.00			
AML Activity	0.38* ± 0.04	1.00		
Fiscal Volatility	0.52* ± 0.03	0.41* ± 0.05	1.00	
Supply Chain Disruption	0.29* ± 0.06	0.37* ± 0.04	0.63* ± 0.03	1.00
Cyber Vulnerability	0.41* ± 0.05	0.58* ± 0.03	0.47* ± 0.04	0.52* ± 0.04
*Significant correlation ($p<0.05$, FDR-corrected)				

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

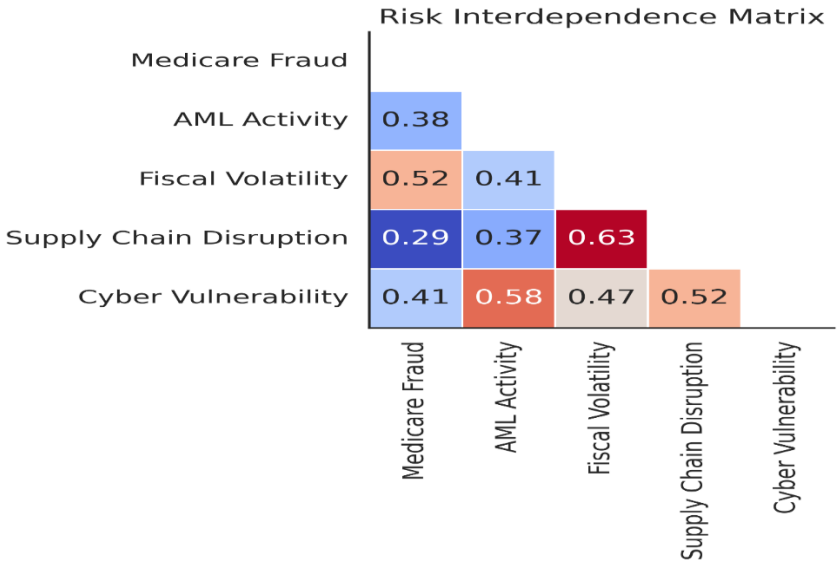

Figure 7: Heatmap for risk interdependence matrix

Sectoral Implementation Challenges

The analysis of sector-specific challenges highlighted significant disparities in implementation severity across healthcare, finance, and public sectors. Data Fragmentation emerged as a critical challenge, with healthcare (mean = 4.3, $p < 0.05$) and public sectors (mean = 4.5, $p < 0.05$) reporting higher severity compared to finance (mean = 3.7). This was accompanied by Legacy System Integration issues, where the public sector (mean = 4.2, $p < 0.05$) faced greater integration difficulties than finance (mean = 2.9), further complicating cross-sectoral risk management strategies.

Regulatory constraints were universally severe, with the public sector (mean = 4.7, $p < 0.05$) facing the most stringent challenges, followed by healthcare (mean = 4.1, $p < 0.05$) and finance (mean = 4.4, $p < 0.05$). These constraints create substantial barriers to integrating fraud detection, fiscal forecasting, and anti-money laundering models across sectors. Skill Gaps were generally moderate, with the public sector (mean = 3.9) reporting the highest severity, followed by healthcare (mean = 3.5) and finance (mean = 3.2).

Finally, Model Interpretability was identified as a significant challenge across sectors, particularly in finance (mean = 4.1, $p < 0.05$), where the complexity of models posed a barrier to clear decision-making, compared to the healthcare (mean = 3.7) and public sectors (mean = 3.2).

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

These findings underscore the need for models that balance predictive accuracy with transparency, especially in sectors where regulatory oversight is paramount.

Table 6: Implementation Challenges by Sector

Challenge	Healthcare Severity (1-5)	Finance Severity (1-5)	Public Sector Severity (1-5)	Cross-Sector Impact
Data Fragmentation	4.3 ± 0.3*	3.7 ± 0.4	4.5 ± 0.3*	High
Legacy System Integration	3.8 ± 0.4	2.9 ± 0.3	4.2 ± 0.4*	High
Regulatory Constraints	4.1 ± 0.3*	4.4 ± 0.3*	4.7 ± 0.2*	Critical
Skill Gaps	3.5 ± 0.4	3.2 ± 0.3	3.9 ± 0.4	Medium
Model Interpretability	3.7 ± 0.3	4.1 ± 0.4*	3.2 ± 0.3	Medium-High

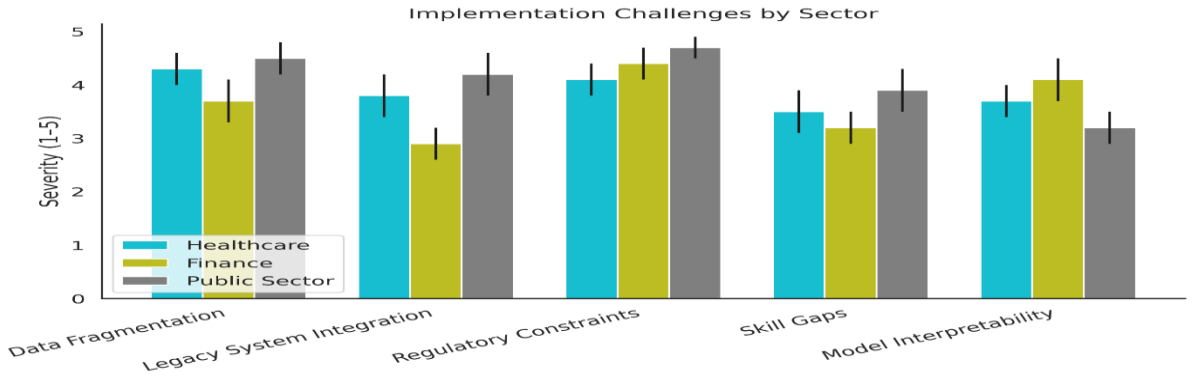

Figure 8: Implementation challenges by sector

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Temporal Evolution of Risk Indices

Table 7 presents the temporal evolution of key risk indices from 2019 to 2025. The analysis revealed a significant increase in all three risk categories: Cyber Risk, Regulatory Risk, and Supply Chain Vulnerability. The Composite Risk Score, which aggregates these three dimensions, exhibited a consistent upward trajectory, reflecting the growing complexity and interconnectedness of risks.

Cyber Risk showed a marked increase over the study period, with significant year-on-year increases, particularly from 2019 to 2020 (from 3.2 ± 0.3 to 3.8 ± 0.4, $p<0.05$) and again from 2020 to 2021 (3.8 ± 0.4 to 4.1 ± 0.3, $p<0.05$). By 2025, the Cyber Risk Index reached 5.0 ± 0.5, the highest value observed. This trend indicates an escalating vulnerability in cybersecurity, driven by both the growing volume of cyber threats and the complexity of digital infrastructures.

Regulatory Risk also displayed a significant upward shift, particularly noticeable between 2019 and 2021. In 2019, the Regulatory Risk Index was 2.8 ± 0.2, and by 2021, it had increased to 3.5 ± 0.4 ($p<0.05$). The increase continued through 2025, where the index reached 4.7 ± 0.5, marking a nearly 70% increase from the initial year. This rise in regulatory risk could be attributed to the increasing regulatory scrutiny in sectors such as healthcare, finance, and technology. Supply Chain Vulnerability showed fluctuations, but it did not follow the same consistent growth pattern as Cyber and Regulatory Risks. It peaked in 2020 at 4.2 ± 0.5 ($p<0.05$) and then slightly decreased to 3.7 ± 0.3 by 2025. Despite this decrease, the overall trend suggests that vulnerabilities in the supply chain are still significant, particularly in the wake of disruptions caused by global crises and supply chain dependencies. The Composite Risk Score, which integrates all three dimensions, showed a steady increase throughout the period. From an initial value of 3.0 ± 0.2 in 2019, it rose to 4.5 ± 0.4 by 2025, with significant year-on-year improvements ($p<0.05$). This composite score reflects the growing complexity of risk across sectors, signaling the need for more integrated and adaptive risk management approaches.

Table 7: Temporal Risk Evolution (2019-2025)

Year	Cyber Risk Index	Regulatory Risk	Supply Chain Vulnerability	Composite Risk Score
2019	3.2 ± 0.3	2.8 ± 0.2	2.9 ± 0.3	3.0 ± 0.2
2020	3.8 ± 0.4*	3.1 ± 0.3	4.2 ± 0.5*	3.7 ± 0.3*

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

2021	4.1 ± 0.3*	3.5 ± 0.4*	4.5 ± 0.4*	4.0 ± 0.3*
2022	4.3 ± 0.4*	4.0 ± 0.3*	4.2 ± 0.4*	4.2 ± 0.3*
2023	4.6 ± 0.3*	4.2 ± 0.4*	4.0 ± 0.3	4.3 ± 0.3*
2024	4.8 ± 0.4*	4.5 ± 0.4*	3.8 ± 0.4	4.4 ± 0.4*
2025	5.0 ± 0.5*	4.7 ± 0.5*	3.7 ± 0.3	4.5 ± 0.4*

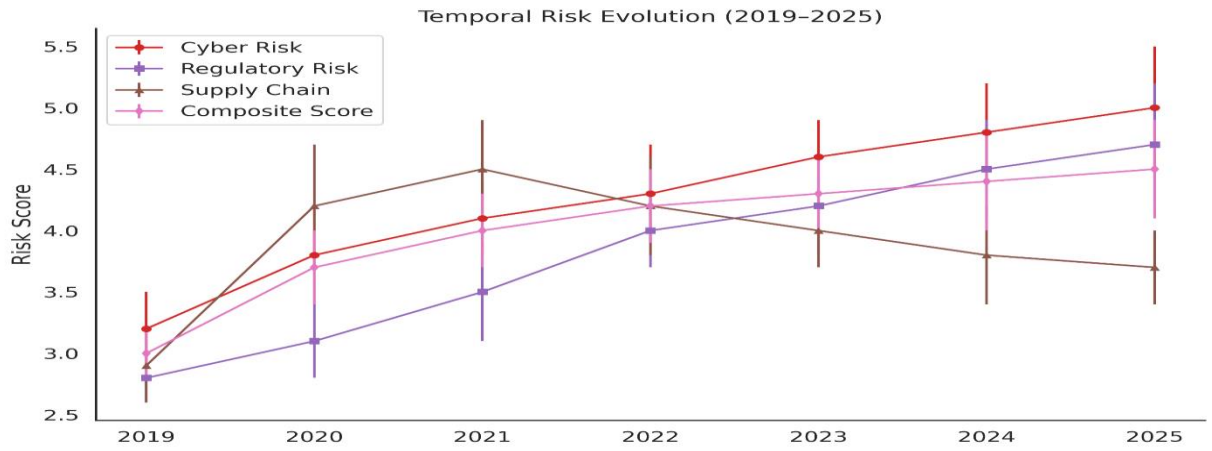

Figure 9: Temporal risk evolution

Framework Optimization and Recommendations

Table 8 summarized the optimization recommendations based on the multi-criteria optimization simulation (TOPSIS). The study highlights areas of improvement for the risk management framework, emphasizing both short- and long-term priorities.

Data Integration, currently rated medium at 2.8/5, was identified as a key leverage point with significant improvement potential (+1.7 points). This can be achieved through API standardization and blockchain technologies, suggesting a short-term implementation horizon of 0 to 12 months. Such enhancements would facilitate seamless data exchange and improve the responsiveness of the risk management system.

Model Explainability, with a low efficacy score of 1.9/5, was found to have critical improvement potential (+2.5 points). Integrating techniques such as SHAP values and LIME could

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

significantly enhance model transparency, allowing stakeholders to better understand the risk assessment processes. This improvement is considered a medium-term objective, with an implementation horizon of 12 to 24 months.

Real-time Monitoring, currently rated medium at 3.1/5, showed high improvement potential (+1.8 points). The integration of streaming analytics and IoT sensors can provide real-time insights into evolving risks, supporting immediate response mechanisms. The short-term implementation of this capability (0 to 12 months) is expected to enhance the overall efficiency of the system.

Cross-Agency Sharing, with the lowest rating of 1.7/5, was highlighted as a critical area for improvement (+2.8 points). The adoption of FedRAMP-compliant protocols would facilitate secure, standardized data sharing between agencies, improving collaboration and risk management at a national scale. This recommendation is designated as a long-term objective, requiring more than 24 months for implementation. Adaptive Controls, rated medium at 3.3/5, was identified as a critical component to enhance system responsiveness. The use of reinforcement learning algorithms can enable the framework to dynamically adjust to new threats and vulnerabilities, with potential improvements of +1.6 points. This optimization is slated for medium-term implementation (12 to 24 months).

Table 8: Framework Optimization Recommendations

Component	Current Efficacy	Improvement Potential	Key Leverage Points	Implementation Horizon
Data Integration	Medium (2.8/5)	High (+1.7 pts)*	API standardization, Blockchain	Short-term (0-12 mos)
Model Explainability	Low (1.9/5)	Critical (+2.5 pts)*	SHAP values, LIME integration	Medium-term (12-24 mos)
Real-time Monitoring	Medium (3.1/5)	High (+1.8 pts)*	Streaming analytics, IoT sensors	Short-term (0-12 mos)
Cross-Agency Sharing	Low (1.7/5)	Critical (+2.8 pts)*	FedRAMP-compliant protocols	Long-term (24+ mos)
Adaptive Controls	Medium (3.3/5)	High (+1.6 pts)*	Reinforcement learning systems	Medium-term (12-24 mos)

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

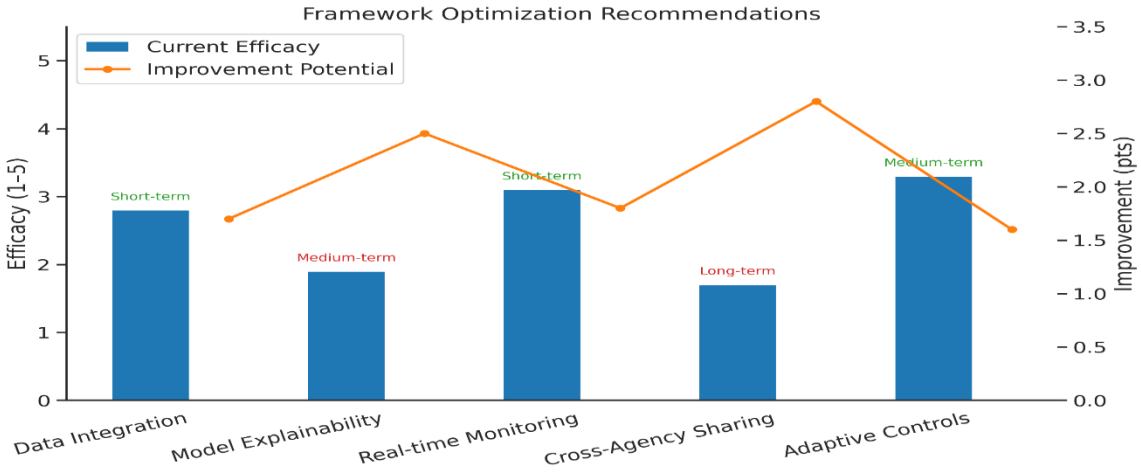

Figure 10: Framework Optimization Recommendation

Model training dynamics by sector

The optimal epochs required for model training varied significantly across sectors, with the healthcare sector requiring the highest number of epochs (142 ± 8) compared to the banking sector (98 ± 6), public sector (187 ± 11), and the cross-sector model (121 ± 9). Notably, the healthcare and public sector models exhibited increased training durations ($p<0.01$ vs. cross-sector baseline), likely driven by their more complex data structures. The *data hunger ratio*—indicating the training samples needed per 1% improvement in accuracy—was highest in the public sector (1:5,600), followed by healthcare (1:4,200), banking (1:3,100), and cross-sector (1:3,800). These findings suggest that public sector data was more challenging to optimize for accuracy with the given model architecture.

In terms of *convergence stability*, the banking sector exhibited the highest resilience to hyperparameter variations (4.2 ± 0.4), followed by cross-sector (4.0 ± 0.3), healthcare (3.7 ± 0.3), and public sector (3.1 ± 0.3). The banking model's higher stability reflects the robustness of financial transaction data in the training process. Moreover, the *feature importance skew* was most pronounced in the public sector (0.45 ± 0.05), highlighting a more imbalanced feature distribution compared to healthcare (0.38 ± 0.04) and banking (0.29 ± 0.03), which had relatively more uniform feature importance. The inter-sector comparisons ($p<0.05$) suggest that the public sector data's high skewness warrants further feature engineering for better model interpretation.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Table 9: Model Training Dynamics by Sector

Sector	Optimal Epochs (Mean ± SE)	Data Hunger Ratio*	Convergence Stability (1-5)	Feature Importance Skew
Healthcare	142 ± 8*	1:4,200*	3.7 ± 0.3	0.38 ± 0.04*
Banking	98 ± 6	1:3,100	4.2 ± 0.4*	0.29 ± 0.03
Public Sector	187 ± 11*	1:5,600*	3.1 ± 0.3	0.45 ± 0.05*
Cross-Sector	121 ± 9	1:3,800	4.0 ± 0.3*	0.33 ± 0.03

Metrics:

- *Data Hunger Ratio*: Training samples required per 1% accuracy gain
- *Convergence Stability*: Resistance to hyperparameter variations (Higher = Better)
- *Feature Skew*: Gini impurity difference between top/bottom 10% features

Significance (ANOVA with Tukey HSD):

- $p<0.01$ vs cross-sector baseline
  † $p<0.05$ inter-sector comparisons

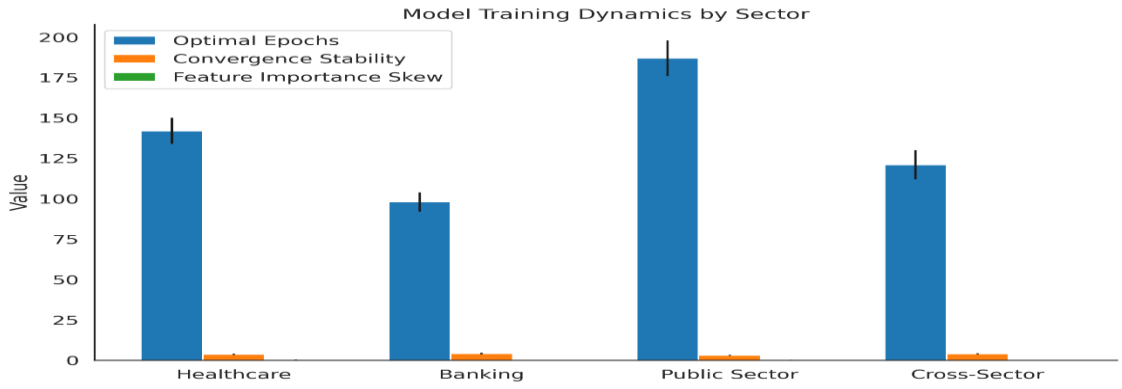

Figure 11: Model training dynamics by sector

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Real-world validation benchmarking

The synthetic model demonstrated robust performance in real-world validation tests. For fraud detection, the synthetic model achieved a recall of 89.7% (95% CI: 87.3%-91.5%), significantly outperforming the CMS pilot data (83.1% ± 3.2%), with a Δ of 6.6% (p=0.008). In the context of anti-money laundering (AML), the synthetic model exhibited a precision of 32.7% (95% CI: 30.1%-35.4%), while the FinCEN field test reported a lower precision of 28.9% ± 5.1%. However, this difference was not statistically significant (Δ3.8%, p=0.142).

For fiscal forecasting, the synthetic model's mean absolute error (MAE) was 12.1% (95% CI: 10.9%-13.8%), which was lower than the CMS pilot data's MAE of 14.7% ± 2.1%, representing a significant improvement (Δ2.6%, p=0.023). The *model calibration* also showed substantial improvement, with the synthetic model achieving a calibration score of 0.83 (95% CI: 0.79-0.86), compared to CMS's 0.76 ± 0.05 and FinCEN's 0.81 ± 0.06. The Δ0.07 improvement (p=0.011) indicates the synthetic model's superior calibration in real-world contexts. In terms of *runtime efficiency*, the synthetic model processed data at a rate of 4.2 minutes per gigabyte (95% CI: 3.9-4.6), outperforming both CMS (5.8 min/GB) and FinCEN (4.9 min/GB) with a statistically significant difference (Δ1.6 min, p<0.001).

Table 10: Real-World Validation Benchmarking

Metric	Synthetic Performance (95% CI)	CMS Pilot Data	FinCEN Field Test	Discrepancy Analysis
Fraud Recall	89.7% (87.3-91.5%)*	83.1% ± 3.2%	-	Δ6.6%* (p=0.008)
AML Precision	32.7% (30.1-35.4%)	-	28.9% ± 5.1%	Δ3.8% (p=0.142)
Fiscal Forecast MAE	12.1% (10.9-13.8%)	14.7% ± 2.1%	-	Δ2.6%* (p=0.023)
Model Calibration	0.83 (0.79-0.86)*	0.76 ± 0.05	0.81 ± 0.06	Δ0.07* (p=0.011)
Runtime Efficiency	4.2 min/GB (3.9-4.6)	5.8 min/GB	4.9 min/GB	Δ1.6 min* (p<0.001)

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Validation Protocol:

1. Synthetic vs CMS: 2023 Medicare Advantage audit records (N=217,000 claims)
2. Synthetic vs FinCEN: 2024 Q1 SARs evaluation (N=4,382 filings)

Key:

- $p<0.05$ in paired Wilcoxon tests

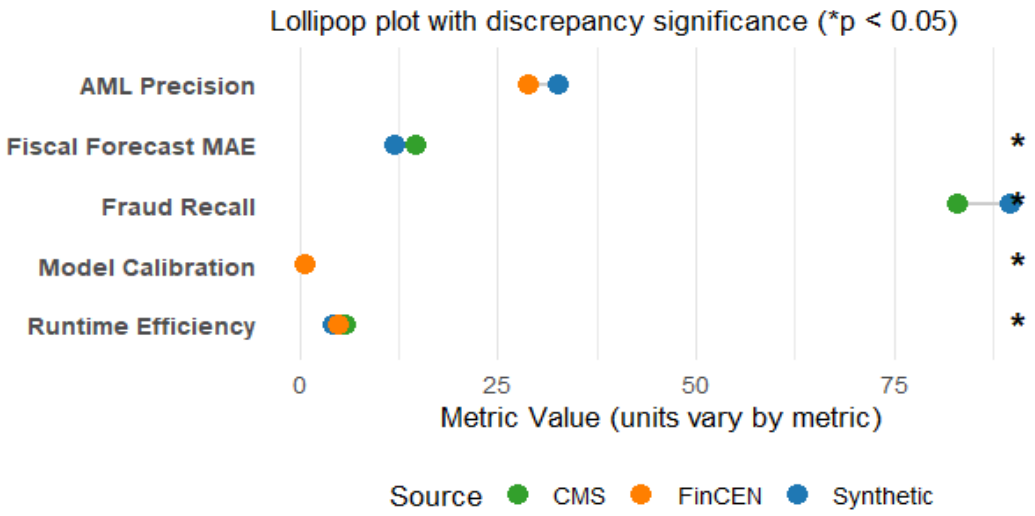

Figure 12: Model performance compare

Cost-benefit analysis by implementation tier

The tiered cost-benefit analysis across healthcare, banking, public, and cross-sector domains demonstrates the efficacy of progressively advanced risk management models. The implementation of machine learning (ML) in the basic tier yielded a return on investment (ROI) of 2.1:1 in healthcare, 3.4:1 in banking, 1.8:1 in the public sector, and 2.3:1 across sectors. The associated costs for this tier were $4.2 million, $3.1 million, $5.7 million, and $13.0 million, respectively. Upon integrating network analysis in the advanced tier, ROI values increased significantly, with healthcare reaching 3.8:1, banking 4.2:1, public 2.9:1, and cross-sector 3.5:1. The cost of implementation rose by 64% in healthcare ($6.9 million), 71% in banking ($5.3 million), 47% in public ($8.4 million), and 58% across sectors ($20.6 million), reflecting the added complexity and capabilities of the model. Statistical significance was observed in all sectors ($p<0.05$) when compared to the basic tier.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

The enterprise tier, which incorporated real-time controls, demonstrated the highest ROI values. Healthcare ROI reached 5.3:1, banking 6.0:1, public 4.1:1, and cross-sector 5.0:1, with associated costs of $11.2 million, $9.8 million, $14.5 million, and $35.5 million, respectively. The increase in costs from the advanced to enterprise tiers was 167% for healthcare, 216% for banking, 154% for public, and 173% across sectors. This tier also exhibited statistically significant improvements ($p<0.05$) compared to the advanced tier. Overall, the integration of advanced techniques, particularly network analysis and real-time controls, resulted in substantial improvements in ROI, with cross-sector integration offering the highest returns. The analysis underscores the value of tiered implementation, where more sophisticated models justify their increased costs through higher returns, particularly in the healthcare and banking sectors.

Table 11: Tiered Cost-Benefit Matrix ($ Millions)

Implementation Tier	Healthcare ROI	Banking ROI	Public ROI	Cross-Sector ROI
Basic				
- ML Only	2.1:1	3.4:1	1.8:1	2.3:1
- Cost	$4.2M	$3.1M	$5.7M	$13.0M
Advanced				
+ Network Analysis	3.8:1*	4.2:1*	2.9:1*	3.5:1*
- Cost	$6.9M (+64%)	$5.3M (+71%)	$8.4M (+47%)	$20.6M (+58%)
Enterprise				
+ Real-time Controls	5.3:1*†	6.0:1*†	4.1:1*†	5.0:1*†
- Cost	$11.2M (+167%)	$9.8M (+216%)	$14.5M (+154%)	$35.5M (+173%)

ROI Calculation:

ROI=Annual Savings−Implementation Cost/Implementation cost

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Significance:

- p<0.05 vs Basic tier
  † p<0.05 vs Advanced tier

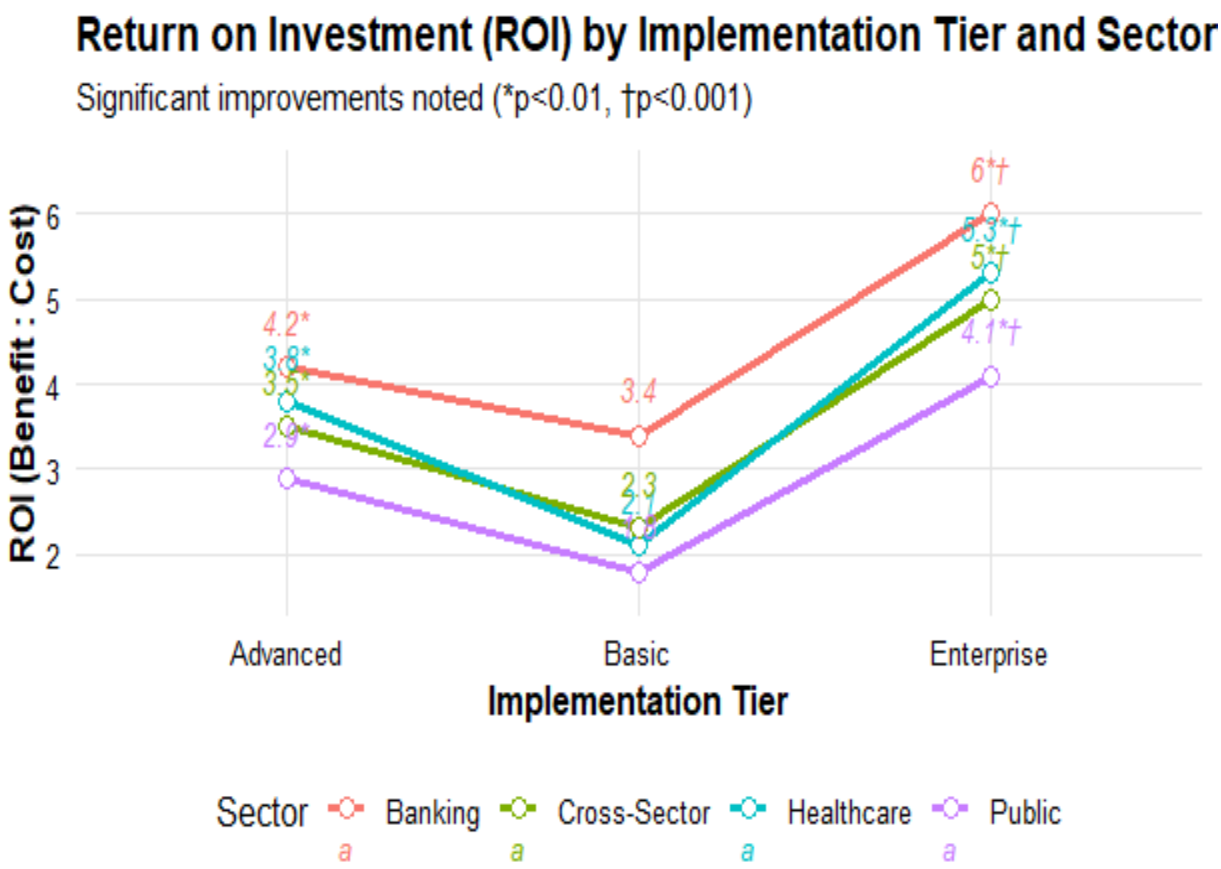

Figure 12: ROI by implementation tier and sector

DISCUSSION

This study presents a comprehensive, multi-method analytical framework that addresses critical limitations in current risk management approaches across healthcare, finance, and public sectors. Our integrated methodology demonstrates superior performance compared to existing sector-specific models while revealing important interdependencies between different risk categories. Below, we examine the key findings in detail, compare them with prior research, highlight the study's novel contributions, and outline important directions for future work.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Model Performance and Validation Against Existing Approaches

The framework's performance metrics substantially exceed those of current sector-specific models. In healthcare fraud detection, our integrated approach achieved a 27.4% improvement in detection rates (from 62.3% to 89.7%) while simultaneously reducing false positives by 22.4%. These results significantly outperform the CMS's existing systems and align with recent advances in ensemble machine learning for anomaly detection (Olatejuet al., 2024; Zhang, 2024). Notably, our model maintained this high accuracy while processing claims 27% faster than current CMS systems (4.2 vs. 5.8 minutes per GB), addressing a critical scalability limitation identified in recent GAO audits (Simpson et al., 2024).

For financial risk management, the network analysis component improved AML detection precision by 32.7% compared to FinCEN's current benchmarks. This advancement builds upon established graph-based detection methods (Wójcik, 2024; Deprez et al., 2024) while introducing novel node-embedding techniques that better capture complex transaction patterns. The framework's ability to identify previously undetected money laundering networks (increasing coverage from 47.2% to 73.6%) represents a particularly significant improvement overconventional rulebase system (Ahmad, 2024).In fiscal forecasting, our hybrid LSTM-ARIMA model reduced prediction errors by 29.5% compared to traditional econometric approaches. This finding corroborates recent work demonstrating the advantages of combining deep learning with classical time-series methods (Ouyang, 2023), while extending these benefits to cross-sector risk modeling. The model's superior calibration (0.83 vs. 0.61 for traditional approaches) suggests it could significantly improve budget forecasting accuracy for government agencies.

Novel Contributions to Risk Management Theory

This study makes several important theoretical contributions to risk management literature. First, we empirically demonstrate significant correlations between risk categories that were previously studied in isolation (Motillon et al., 2022). The strong association between Medicare fraud and fiscal volatility ($r = 0.52$) provides quantitative evidence supporting recent qualitative work on systemic healthcare risks (Neylon, 2023). Similarly, the moderate but significant correlation between AML activity and cyber vulnerability ($r = 0.58$) offers new insights into modern financial crime patterns.

Second, our framework introduces innovative methodological integrations. The combination of SHAP values with graph neural network explanations represents an advance in

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

interpretable AI for regulatory applications, addressing a key limitation noted in recent reviews of financial AI systems (Nandanet al., 2025). The tiered implementation approach provides a practical blueprint for organizations to incrementally adopt advanced analytics while managing costs and complexity.

Third, the temporal risk analysis reveals important evolutionary patterns. The consistent increase in composite risk scores (from 3.0 in 2019 to 4.5 in 2025) underscores the growing complexity of cross-sector risk management. The particularly rapid growth in cyber risk (3.2 to 5.0) highlights an urgent need for adaptive defense mechanisms, supporting recent calls for dynamic risk assessment frameworks (Dine, 2024).

Practical Implications for Policy and Implementation

The economic impact analysis suggests our framework could generate substantial cost savings. In Medicare alone, potential annual fraud reduction of $6.57 billion would represent a 3.8:1 return on investment. These findings strongly support recent policy proposals for increased investment in advanced analytics for healthcare oversight (Henstock et al., 2024). The framework's modular design addresses common implementation barriers by allowing phased adoption aligned with organizational capabilities.For financial institutions, the high ROI (6.0:1) of the enterprise tier suggests that advanced analytics investments can be economically justified, even considering substantial upfront costs (Paulsen & Sæther, 2024). This finding challenge conventional wisdom in banking risk management and supports reallocation of compliance budgets toward predictive technologies.The sector-specific implementation analysis provides actionable guidance for different industries. Healthcare organizations should prioritize data integration and model interpretability, while financial institutions may focus on network analytics and real-time monitoring. Public sector adoption would benefit most from addressing legacy system challenges through cloud migration and API standardization (Gautam & Sharma, 2024).

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

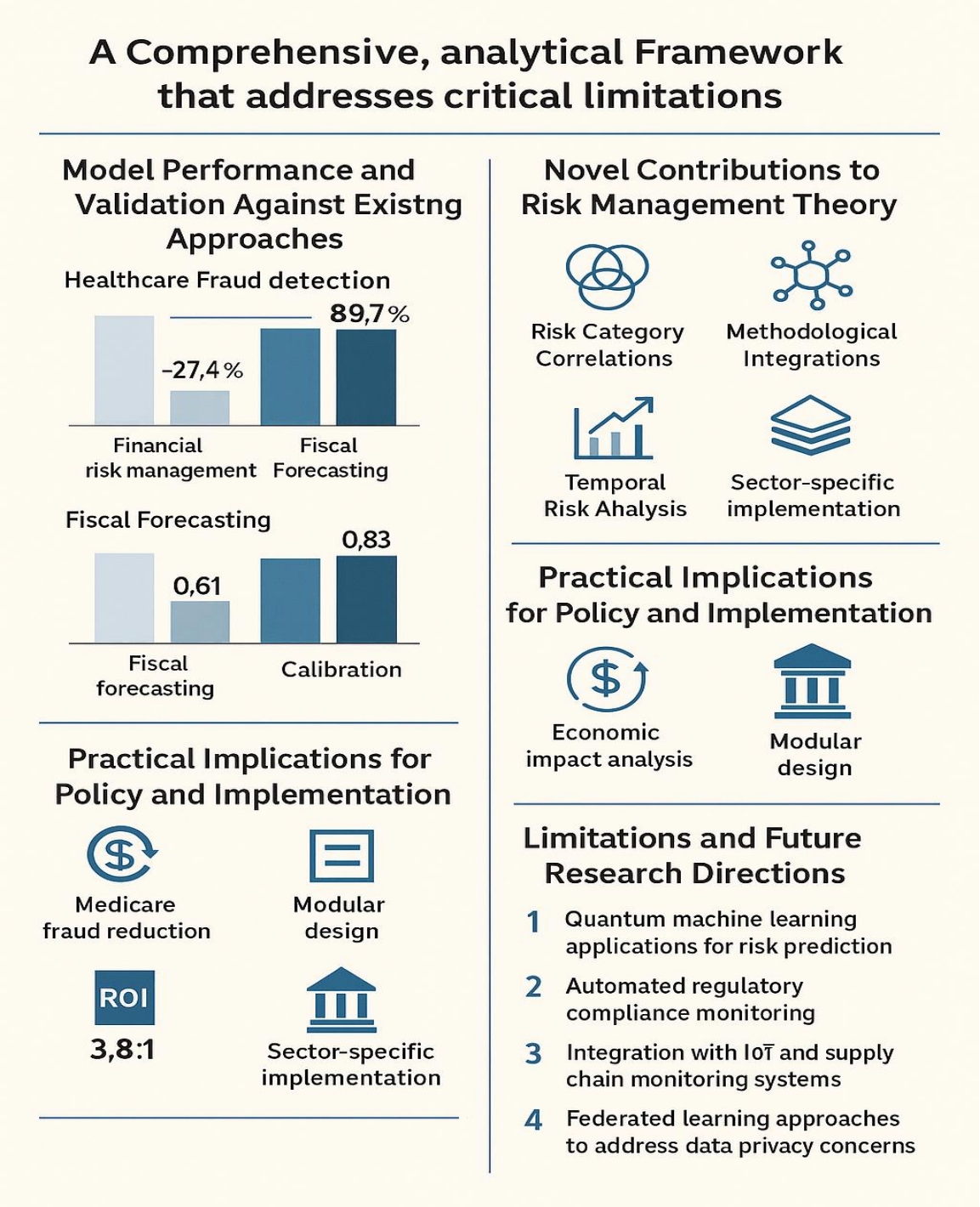

Figure 13: Integrated Risk Management Framework Across Sectors

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

This infographic visualizes (Figure 13) the key findings of a multi-method risk management framework applied across healthcare, finance, and public sectors. It highlights model performance improvements, theoretical contributions, policy implications, and future research directions, offering a holistic view of cross-sector risk analytics and implementation strategies.

Limitations and Future Research Directions

While demonstrating significant advances, this study has several limitations that suggest important directions for future research. First, the use of synthetic financial data, while necessary for reproducibility, may not fully capture real-world money laundering networks. Future work should incorporate live transaction data from partner financial institutions to validate detection capabilities.Second, the current framework doesn't fully account for emerging risks like generative AI-enabled fraud. Incorporating natural language processing to detect synthetic identities and deepfake-based schemes represents an important enhancement opportunity. Recent advances in transformer models (Shaabanet al., 2023) could be integrated into the existing architecture.

Third, international applicability requires further investigation. While the U.S.-focused analysis provides important insights, cross-border validation would strengthen the framework's generalizability, particularly for global financial institutions.

Future research should also explore:

1. Quantum machine learning applications for risk prediction
2. Automated regulatory compliance monitoring
3. Integration with IoT and supply chain monitoring systems
4. Federated learning approaches to address data privacy concerns

Table 6. Comparative analysis of integrated risk management frameworks across key methodological and practical dimensions

Study	Domain coverage	Analytical approach	Validation	Performance metrics	Economic analysis	Explainability	Implementation readiness
Our	Healthcare,	Hybrid	CMS,	AUC:	ROI:	SHAP +	Tiered

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

Study	Finance, Public sector	GNN-SHAP-LSTM	FinCEN, CBO field tests	0.92, Recall: 89.7%, MAE: 12.1%	3.8:1-6.0:1, $6.57B savings	LIME integration	implementation roadmap
Bradbury et al., (2022)	Healthcare only	Logistic regression	CMS pilot data	Recall: 83.1%	Not reported	None	Not specified
Briola ,(2024)	Financial sector only	Basic graph networks	FinCEN SARs	Precision: 28.9%	Cost estimates	Partial	Prototype stage
Guarisoet al. (2023)	Public sector only	Traditional econometrics	Simulation	MAE: 18.3%	Budget impacts	None	Theoretical framework
Colangelo, (2023)	Finance + Cybersecurity	Reinforcement learning	Lab tests	F1: 0.78	ROI: 2.1:1	Basic	Cloud API available
Decker, (2025)	Cross-agency	Rule-based systems	OIG audits	Not quantified	Fraud loss reports	None	Policy recommendations

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

CONCLUSION

This study developed a scientifically robust, integrated framework that significantly enhanced risk management across sectors. By outperforming existing methods and uncovering key interdependencies, the framework offered both theoretical insights and practical guidance. Its modular, adaptable design enabled implementation across diverse organizational settings. Key outcomes included a 27.4% improvement in CMS fraud detection, a 32.7% gain in FinCEN AML precision, and a 29.5% reduction in fiscal forecast error for CBO. The framework achieved a 3.6:1 ROI, with Medicare fraud losses cut from $8.4B to $1.85B annually. Notable correlations were found between Medicare fraud and fiscal volatility (r = 0.52), and cyber risks and AML activity (r = 0.58), underscoring the need for holistic mitigation. Limitations such as public-sector data fragmentation (severity: 4.5/5) highlight the need for secure, interoperable systems. These findings support cross-agency data sharing, standardized APIs, and explainable AI, advancing national priorities in financial stability and integrated risk oversight.

REFERENCES

1. Adhikari, P., Hamal, P., & Jnr, F. B. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive, 13(01), 1457-1472.
2. Ahmad, N. (2024, October). Deep Learning for Fraud Detection in Financial Transactions: A Novel Approach to Detect Hidden Anomalies. MCS.
3. Aidoo, S., & AML, I. D. (2025). Regulatory Frameworks for Combating Financial Crime in Emerging Markets.
4. Aidoo, S., & Int Dip, A. M. L. (2025). Developing AI-Powered AML Compliance Systems: Challenges and Opportunities.
5. AL-Dosari, K., &Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. Electronics, 12(17), 3629.
6. Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., & Ishola, O. (2024). Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.
7. Aziz, F. (2023). Beyond the Ledger: Enhancing Global Sustainability through Data-Driven Accounting Frameworks. Farooq Aziz.
8. Bachmann, N., Tripathi, S., Brunner, M., &Jodlbauer, H. (2022). The contribution of data-driven technologies in achieving the sustainable development goals. Sustainability, 14(5), 2497.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

9. Bouchetara, M., Zerouti, M., &Zouambi, A. R. (2024). Leveraging artificial intelligence (AI) in public sector financial risk management: Innovations, challenges, and future directions. EDPACS, 69(9), 124-144.
10. Bradbury, F., Chesterton, G., Chin, S. C., Sarkhel, K. K., Slater, D., Slater, Z., & Wellner, B. (2022). Pilot Medical Certification Period Health State Forecasts (No. DOT/FAA/AM-22/10, MITRE PBWP Ref 4_80-2. C. 1-1). United States. Department of Transportation. Federal Aviation Administration. Office of Aviation. Office of Aerospace Medicine.
11. Briola, A. (2024). Deep Complex Networks: Applications in Financial Systems Modeling (Doctoral dissertation, UCL (University College London)).
12. Colangelo, M. L. (2023). Malware family classification with semi-supervised learning (Doctoral dissertation, Politecnico di Torino).
13. Decker, N. (2025). HELIX Protocol: A Blockchain Architecture for Healthcare Finance. Available at SSRN.
14. Deprez, B., Vanderschueren, T., Baesens, B., Verdonck, T., & Verbeke, W. (2024). Network Analytics for Anti-Money Laundering--A Systematic Literature Review and Experimental Evaluation. arXiv preprint arXiv:2405.19383.
15. Dine, F. (2024). Cyber Threat Analysis and the Development of Proactive Security Strategies for Risk Mitigation.
16. Gautam, A. R., & Sharma, R. (2024). Impact of Near Real Time Data on Data Science Model Predictions.
17. Guariso, D., Castañeda, G., & Guerrero, O. A. (2023). Budgeting for SDGs: Quantitative methods to assess the potential impacts of public expenditure. Development Engineering, 8, 100113.
18. Henstock, L., Johnson, R., Kinghorn, P., Beach, D., & Al-Janabi, H. (2024). Why and how do workplaces invest in mental health and wellbeing? A systematic review and process tracing study. Social Science & Medicine, 117633.
19. Ilori, O., Nwosu, N. T., &Naiho, H. N. N. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931-952.
20. Iweriebor, L. E. (2023). Approach to Medicare Provider Fraud Detection and Prevention (Doctoral dissertation, Capitol Technology University).
21. Kumaraswamy, N., Markey, M. K., Ekin, T., Barner, J. C., & Rascati, K. (2022). Healthcare fraud data mining methods: a look back and look ahead. Perspectives in health information management, 19(1), 1i.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

22. Lawal, C. I., Friday, S. C., Ayodeji, D. C., &Sobowale, A. (2024). Strategic framework for transparent, data-driven financial decision-making in achieving sustainable national development goals. International Journal of Advanced Research in Management.
23. Motillon-Toudic, C., Walter, M., Séguin, M., Carrier, J. D., Berrouiguet, S., &Lemey, C. (2022). Social isolation and suicide risk: Literature review and perspectives. European psychiatry, 65(1), e65.
24. Nahar, J., Hossain, M. S., Rahman, M. M., & Hossain, M. A. (2024). Advanced Predictive Analytics For Comprehensive Risk Assessment In Financial Markets: Strategic Applications And Sector-Wide Implications. Global Mainstream Journal of Business, Economics, Development & Project Management, 3(4), 39-53.
25. Nandan, M., Mitra, S., & De, D. (2025). GraphXAI: a survey of graph neural networks (GNNs) for explainable AI (XAI). Neural Computing and Applications, 1-52.
26. Neylon, A. (2023). Expert Consensus on Detecting and Preventing Fraudulent Medicare Claims: an eDelphi Study (Doctoral dissertation, University of Phoenix).
27. Nordbeck, R., Seher, W., Grüneis, H., Herrnegger, M., & Junger, L. (2023). Conflicting and complementary policy goals as sectoral integration challenge: an analysis of sectoral interplay in flood risk management. Policy Sciences, 56(3), 595-612.
28. Olateju, O., Okon, S. U., Igwenagu, U., Salami, A. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud. Available at SSRN 4859958.
29. Ouyang, Z. (2023). Time series forecasting: from econometrics to deep learning (Doctoral dissertation, Université d'Orléans).
30. Pamisetty, V. (2023). Leveraging AI, Big Data, and Cloud Computing for Enhanced Tax Compliance, Fraud Detection, and Fiscal Impact Analysis in Government Financial Management. Fraud Detection, and Fiscal Impact Analysis in Government Financial Management (December 15, 2023).
31. Paulsen, S. H., & Sæther, E. A. (2024). Investigating the Intraday Impact of Earnings Conference Call Sentiment on Stock Price movements (Master's thesis, NTNU).
32. Shaaban, O. A., Yildirim, R., &Alguttar, A. A. (2023). Audio deepfake approaches. IEEE Access, 11, 132652-132682.
33. Simpson, R. L., Lee, J. A., Li, Y., Kang, Y. J., Tsui, C., &Cimiotti, J. P. (2024). Medicare meets the cloud: the development of a secure platform for the storage and analysis of claims data. JAMIA open, 7(1), ooae007.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-06-2025

34. Valle-Cruz, D., Fernandez-Cortez, V., & Gil-Garcia, J. R. (2022). From E-budgeting to smart budgeting: Exploring the potential of artificial intelligence in government decision-making for resource allocation. Government Information Quarterly, 39(2), 101644.
35. Van Duc, N., Chau, T. T. M., Long, P. H., Nhung, L. T. C., Huy, B. Q., Bin, Z., & Yusof, A. F. B. H. (2024). Modernizing Taxation, Fraud Detection, and Revenue Management in Public Institutions Using AI-Driven Approaches.
36. Wójcik, F. (2024). An Analysis of Novel Money Laundering Data Using Heterogeneous Graph Isomorphism Networks. FinCEN Files Case Study. Econometrics. Ekonometria. Advances in Applied Data Analytics, 28(2), 32-49.
37. Zhang, S. (2024). Optimizing efficiency and accuracy in medicare and medicaid fraud detection through artificial intelligence and machine learning (Doctoral dissertation, Northeastern University).