

Assessing the Impact of Machine Learning Model on Identifying Terrorism Financing Patterns within the U.S. Financial Industry

Victor Boateng¹, Elizabeth Kuukua Amoako², Mildred Adwubi Bonsu³,
Matthew Oman-Amoako⁴

¹Department of Business Administration & Business Analytics, East Tennessee State University, USA

²Naveen Jindal School of Management, University of Texas, Dallas, USA

³University at Albany, State Univ. Of New York

⁴Department of Business Administration, Accra Institute of Technology, Ghana

Abstract

The increasing complexity and sophistication of terrorism financing have outpaced traditional monitoring systems within the U.S. financial industry, creating a need for more advanced, data-driven detection tools. Although machine learning (ML) is widely recognized for its potential to improve anomaly detection and behavioral profiling, there is limited empirical research on its actual application and effectiveness in fighting terrorism financing. This paper aims to carefully evaluate how machine learning models are currently used in U.S. financial institutions to identify terrorism financing patterns and whether these efforts contribute meaningfully to achieving Goal 16 of the United Nations Sustainable Development Goals (Peace, Justice, and Strong Institutions). A qualitative research approach was used, including a thorough review of empirical studies, existing literature, industry cases, and analysis of documents from regulatory agencies and industry white papers. Our findings show that though ML shows promise in recognizing patterns and enabling early detection, its implementation is heavily limited by regulatory compliance requirements, privacy laws, technological fragmentation and institutional risk aversion. Additionally, most institutions lack access to timely and adequate training data, especially for rare or evolving threat scenarios. The study concludes that the current environment in the U.S. financial sector leads to a performance-constrained calibration of machine learning models, where institutional, legal and infrastructural barriers prevent full optimization. Therefore, achieving the full potential of ML in this area will require more collaborative frameworks among regulators, institutions, and technology providers, along with standardized data-sharing protocols and national-level integration strategies.

Keywords: Machine Learning, Terrorism Financing, U.S. Financial Sector, Anti-Money Laundering (AML), Regulatory Compliance

Introduction

The September 11, 2001, terrorist attacks fundamentally transformed the landscape of financial crime prevention in the United States, which catalyzed a paradigmatic shift toward technologically mediated surveillance and detection mechanisms within the financial services sector (Boateng et al. 2025). In the

subsequent decades, the evolution of terrorism financing methodologies has paralleled advances in digital financial infrastructure, which has created increasingly sophisticated channels for illicit fund transfers that challenge traditional detection paradigms (Parker, 2014). The contemporary terrorism financing ecosystem operates through a complex network of formal and informal financial channels, exploits regulatory arbitrage opportunities and technological innovations to obscure transactional patterns and evade detection systems (Brown, 2017).

The United Nations' adoption of the 2030 Agenda for Sustainable Development has established a comprehensive framework for addressing global security challenges through multilateral cooperation and technological innovation (Carpentier & Braun, 2020). The seventeen Sustainable Development Goals (SDGs), ratified by the UN General Assembly in 2015, represent an ambitious global compact that tackles interconnected social, economic, and environmental challenges (Leal Filho et al, 2019). Relevant to this research is SDG 16, which explicitly calls for the promotion of peaceful and inclusive societies, access to justice for all, and the establishment of effective, accountable institutions at all levels (United Nations, 2019). The relationship between economic development and crime reduction, as shown by empirical research indicating negative correlations between economic prosperity and criminal activity (Jackson et al. 2018), which highlights the importance of effective counter-terrorism financing mechanisms in achieving broader developmental objectives.

According to Zoli et al. (2018), the financial dimension of terrorism represents a significant vulnerability that, when effectively targeted, can significantly disrupt terrorist operational capabilities. Contemporary estimates suggest that global terrorism financing generates substantial illicit revenues through diversified criminal enterprises, including human trafficking operations that generate approximately \$150.2 billion annually through forced labor, sexual exploitation, and organ harvesting (Broad et al., 2022). These financial flows provide the material foundation for terrorist operations and facilitate the complex logistical networks required for planning, executing and sustaining terrorist activities across geographic boundaries (Byrne et al. 2020).

The U.S. financial industry's response to terrorism financing threats has been marked by the progressive adoption of technological solutions, particularly machine learning algorithms designed to enhance pattern recognition capabilities within vast datasets of financial transactions. This technological evolution reflects broader trends in the digitization of financial services and the increasing availability of computational resources capable of processing complex algorithmic models (Nwoke, 2024). However, the implementation of machine learning systems for terrorism financing detection operates within a complex socio-technical environment defined by regulatory requirements, institutional constraints, technological limitations, and operational considerations that collectively shape the effectiveness of these systems.

Literature Review

The role of financial profiling in the international fight against crime

The proliferation of terrorism financing through sophisticated financial networks has positioned machine learning technologies as crucial tools in the U.S. financial industry's counter-terrorism efforts (Brooks et al. 2025). Their implementation reveals core challenges that set terrorism financing detection apart from conventional anti-money laundering operations. Unlike traditional financial crimes that display relatively predictable behavioral patterns, terrorism financing includes a diverse range of activities, from the laundering of illicitly obtained funds to the legitimate sourcing of money later funnelled to terrorist operations, including charitable donations to organizations supporting extremist activities (Mekpor, 2019).

This complexity is further complicated by the multi-actor nature of terrorism financing networks, which involves individual operatives. These sophisticated, organized groups with dedicated financial infrastructures employ hybrid models to simultaneously engage in multiple criminal enterprises, including human trafficking, bribery and tax evasion (Azzahra, 2025). The dynamic and adaptive nature of these financing patterns, illustrated by the rapid transition to digital payment systems and cryptocurrency platforms following traditional banking scrutiny, requires machine learning models that can detect emerging behavioral signatures, however, considering the vast phenomenological scope of terrorism financing activities within the heavily regulated U.S. financial environment.

According to Canhoto (2021), the deployment of machine learning systems for terrorism financing detection within U.S. financial institutions faces unprecedented technical and regulatory challenges that significantly impact model effectiveness and operational viability. The inherent difficulty in validating ML model performance is exacerbated by the extended temporal lag between suspicious activity identification and formal law enforcement investigation outcomes, often spanning multiple years (Amoah et al. 2025). Terrorism financing methodologies evolve rapidly in response to detection efforts and external factors such as regulatory changes or geopolitical events (Horobets et al. 2025). This temporal disconnect forces financial institutions to engage in speculative modeling whilst processing vast volumes of heterogeneous data streams, including structured transaction records, unstructured customer communications, biometric authentication data and digital interaction logs, which require substantial technological investments estimated at billions of dollars annually across the U.S. banking sector. Moreover, the stringent regulatory framework governing U.S. financial institutions, particularly requirements for algorithmic transparency, non-discriminatory customer treatment and comprehensive audit trails mandated by federal banking regulators and national security agencies. This creates significant barriers to adopting sophisticated machine learning architectures such as deep neural networks or ensemble methods whose decision-making processes lack interpretability. Conceptually, these regulatory constraints, though essential for protecting customer rights and ensuring accountability in national security applications, fundamentally limit the types of ML algorithms that can be deployed in terrorism financing detection. This thus potentially constrains the industry's ability to leverage the full potential of artificial intelligence technologies in counter-terrorism finance operations.

Theoretical Framework: Affordances Theory in Machine Learning Applications for Terrorism Financing Detection

The effectiveness of machine learning in detecting terrorism financing patterns cannot be understood by looking only at technology or only at organizations. Instead, we need a framework that considers both technical and social factors. This study uses the theory of affordances, developed by Gibson (1979) and later applied to information systems by researchers like Leonardi (2013) and Volkoff and Strong (2013). Affordances theory examines how technology properties interact with user characteristics to create possibilities for action. In the context of terrorism financing detection, this means understanding how machine learning capabilities such as pattern recognition and data processing work together with organizational factors like regulatory requirements, staff expertise and institutional goals to achieve core objectives. The theory focuses on what users can do with the technology, not just what the technology can theoretically accomplish.

The theory of affordances demonstrates that technology outcomes depend on how organizations recognize and utilize technological capabilities. Many contextual factors, including regulatory frameworks, security

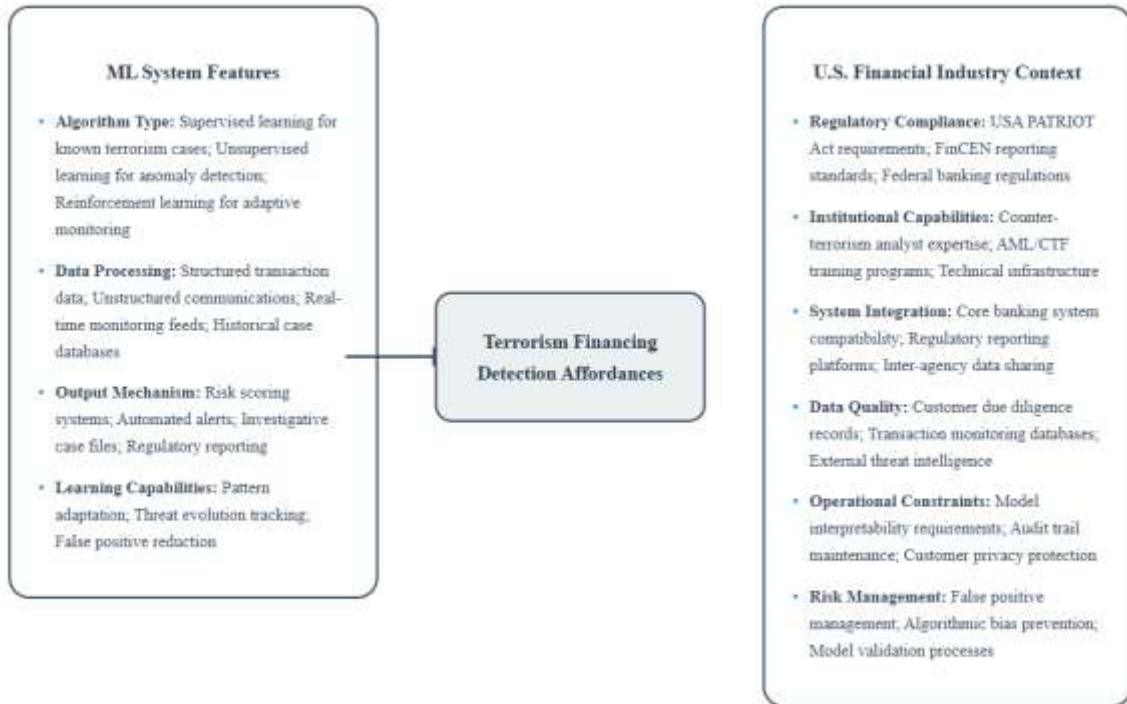
protocols, training programs, and strategic goals, shape this process. For the detection of terrorism financing in U.S. financial institutions, this means that the success of machine learning relies on both algorithm characteristics, such as transparency and accuracy, and organizational traits, including compliance structures and analyst skills. The theory rejects simple explanations that solely blame either technological limitations or organizational issues. Instead, it explores how technical capabilities and institutional practices interact over time. This approach helps explain why some financial institutions succeed more than others in using machine learning for terrorism financing detection, even when applying similar technologies.

The Technological Affordances of Machine Learning in Terrorism Financing Detection

Machine learning technologies offer significant potential for detecting terrorism financing patterns within U.S. financial institutions by processing large volumes of structured and unstructured data to identify hidden relationships and anomalous behaviors (Kumar & Singh, 2024). According to Gheisari et al. (2017), these systems differ from traditional programming because they discover patterns in data rather than following predetermined rules. This capability allows financial institutions to identify previously unknown terrorism financing methods across various data sources, including transaction records, customer communications and behavioral indicators. Mbiva & Correa (2024) noted that three main types of machine learning approaches can be applied to terrorism financing detection. Supervised learning works best when there are known examples of terrorism financing cases that can be used to train the system. Unsupervised learning is useful for discovering unusual transaction patterns when the specific indicators are not known in advance. Reinforcement learning can help create adaptive monitoring systems that improve over time as they encounter new threats (Shehzadi, 2024). However, the choice of which approach to use is often limited by practical considerations such as staff expertise, regulatory requirements, available computing power and system compatibility rather than which method would work best theoretically.

The success of machine learning systems in detecting terrorism financing depends heavily on having access to high-quality, representative data for training and operation. Financial institutions face significant challenges in collecting comprehensive datasets because terrorism financing cases take months or years to be fully investigated and confirmed by law enforcement (Canhoto, 2021). This creates a shortage of validated examples that can be used to train supervised learning systems effectively. Additionally, Westgard & Westgard (2016) underscored that combining data from different sources creates problems with standardization and quality control that can limit system performance. Although machine learning systems can learn and adapt over time, this capability also introduces risks, including the development of feedback loops that reinforce biases or mistakes. Inferences from the literature showed that these systems can become so complex that analysts cannot understand how they make decisions, which conflicts with regulatory requirements for transparent and explainable decision-making in counter-terrorism operations. The quality of training data is particularly important because poor data can lead to unreliable results, and this problem is worse when using external data sources where financial institutions cannot verify the underlying assumptions or collection methods. These technical and operational challenges show that the effectiveness of machine learning in terrorism financing detection depends on how well the technology fits with the specific requirements and constraints of U.S. financial institutions.

Figure 1. The Relationship Between Machine Learning Features, Contextual Factors, and System Affordances in Terrorism Financing Detection within U.S. Financial Institutions



This framework illustrates how machine learning system features interact with U.S. financial industry contextual factors to create specific affordances for terrorism financing detection and prevention.

(Montasari 2024).

The framework in Figure 1 shows how machine learning (ML) system features connect with the real-world context of the U.S. financial industry to influence the tools available for detecting terrorism financing. In this paper, the figure highlights that the success of ML systems depends on technical aspects, such as algorithm type (supervised, unsupervised, reinforcement), data processing abilities, and learning flexibility, and on institutional factors like regulatory compliance, data quality, system integration and risk management procedures. ML’s ability to recognize changing terrorism financing tactics depends greatly on high-quality data (like transaction monitoring and due diligence records) and strong regulatory frameworks such as the USA PATRIOT Act and FinCEN standards. At the same time, industry-specific limitations like model interpretability, auditability, and privacy protection restrict how far ML can be implemented. This combined view emphasizes that any evaluation of ML’s impact must consider the interaction between the models’ technical potential and the institutional environment where they are used, ensuring detection methods are both practical and legally compliant.

Research Design and Methodological Approach

This study uses a qualitative case study methodology to examine how U.S. financial institutions implement machine learning technologies for terrorism financing detection. The case study approach is well-suited for this research because it allows the researchers to understand how technological change occurs within specific organizational contexts. This methodology is especially suitable for studying algorithm development because it helps eliminate false correlations that might obscure which variables are used and

why they are chosen. The qualitative design enables in-depth exploration of the contextual factors influencing the effectiveness of machine learning in terrorism financing detection. These factors include regulatory requirements, organizational culture, staff expertise and institutional attitudes toward risk.

Findings

The implementation of machine learning algorithms in terrorism financing detection within the U.S. financial sector represents a significant evolution in counter-terrorism financing (CTF) methodologies, which necessitates rigorous empirical assessment of their efficacy and regulatory compliance implications. Contemporary financial institutions have increasingly adopted supervised learning approaches that leverage historical conviction data and court production orders to develop algorithmic models capable of identifying suspicious transaction patterns and customer behavioral anomalies. However, the inherent limitations of training datasets, characterized by temporary delays between criminal activity and judicial outcomes, legal constraints on information disclosure and the specificity of criminal behaviors that resist generalization, pose significant challenges to model development and validation. According to Horobets et al. (2025), the deployment of these ML-based detection systems operates within a complex regulatory framework established by the USA PATRIOT Act and Bank Secrecy Act amendments creates tension between technological innovation imperatives and compliance. These obligations simultaneously address the adaptive nature of terrorist financing networks that continuously evolve to circumvent detection mechanisms.

The assessment of ML model impact on terrorism financing identification reveals a paradoxical landscape wherein algorithmic sophistication enhances pattern recognition capabilities; however, it simultaneously introduces new vulnerabilities related to algorithmic bias, false positive rates and interpretability requirements mandated by regulatory oversight bodies.

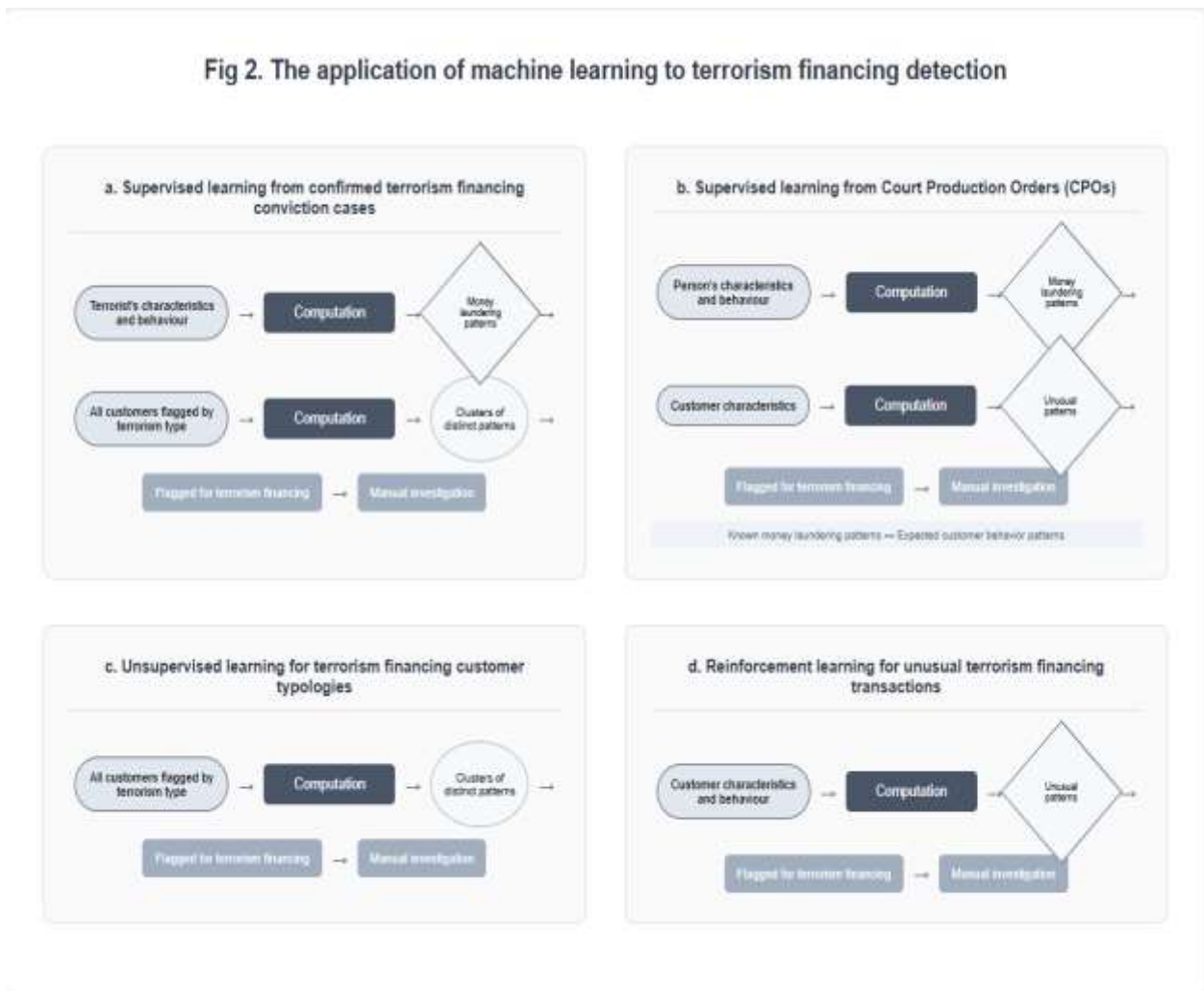
Findings from the empirical studies revealed that financial institutions must navigate the challenges inherent in supervised learning approaches that rely on confirmed criminal conviction data, which often reflects unique behavioral patterns such as the geographical clustering of al-Qaeda affiliates in specific postal codes and their association with business typologies. This may not generalize across diverse terrorist financing methodologies employed by different organizations. The reactive nature of the court production order-based model training further compounds these limitations. However, institutions develop algorithms based on post-hoc analysis of flagged accounts rather than proactive identification capabilities. Consequently, the efficacy of ML models in terrorism financing detection must be evaluated not merely through traditional performance metrics such as precision and recall, but through a comprehensive framework that incorporates regulatory compliance costs, operational efficiency gains, risk mitigation effectiveness, and the dynamic adaptability required to address evolving terrorist financing strategies in an increasingly digitized financial ecosystem.

Empirical Material Collected

Instrument	Data Collected
Documents (including electronic files)	<ul style="list-style-type: none">• Machine learning algorithm specifications and model documentation• Terrorism financing detection queries and rule sets• Suspicious Activity Report (SAR) filing protocols and templates• Financial Crimes Enforcement Network (FinCEN) guidance documents• Model validation reports and performance metrics

	<ul style="list-style-type: none"> • Internal compliance policies for CTF/AML operations • Training datasets and feature engineering documentation • Regulatory examination reports and findings
Interviews	<ul style="list-style-type: none"> • Compliance Officers: 6 • ML Engineers and Data Scientists: 8 • Financial Intelligence Unit Analysts: 7 • Risk Management Directors: 3 • Regulatory Affairs Specialists: 4
Observations	<ul style="list-style-type: none"> • Model development workshops: 4 × 2-hour sessions • SAR review committee meetings: 6 × 1.5-hour sessions • Algorithm performance monitoring: 8 × 1-hour sessions • Regulatory compliance audits: 3 × 4-hour sessions

Fig 2. The application of machine learning to terrorism financing detection



(Montasari 2024).

Figure 2 illustrates the diverse applications of machine learning (ML) models in detecting terrorism financing activities within financial systems, which emphasizes four distinct learning approaches. Supervised learning (panels a and b) leverages labeled data from confirmed terrorism financing cases and

Court Production Orders (CPOs) to identify money laundering and behavioral patterns by computing and clustering customer characteristics and behaviors. Unsupervised learning (panel c) focuses on detecting unknown or emerging terrorism financing typologies by identifying clusters among customers flagged by terrorism indicators without prior labels. Finally, reinforcement learning (panel d) adapts to evolving threats by continuously analyzing customer transactions to detect unusual patterns in real-time. Across all methods, the computational output flags potential terrorism financing for further manual investigation, demonstrating how ML enhances both pattern recognition and proactive threat detection in complex financial environments.

Impact of Machine Learning Models on Identifying Terrorism Financing Patterns within the U.S. Financial Industry.

The epistemological foundations of machine learning applications in terrorism financing detection within the U.S. financial sector reveal fundamental tensions between algorithmic sophistication and evidentiary constraints that characterize contemporary counter-terrorism financing (CTF) operations. (Montasari, 2024). The deployment of supervised learning methodologies utilizing Court Production Orders (CPOs) as training datasets exemplifies this tension, wherein the temporary advantages of more frequent and timely data acquisition are systematically undermined by the inherent uncertainty regarding the criminal nature of investigated activities and their ultimate judicial outcomes. This evidential ambiguity creates what can be conceptualized as a "probabilistic training paradox," where the algorithmic models are calibrated on datasets of uncertain criminal provenance, potentially encoding false positives into the foundational learning architecture. Furthermore, the reliance on unsupervised learning approaches for customer behavioral clustering, while circumventing the limitations of historical conviction-based datasets, operates under the problematic assumption of behavioral divergence between legitimate and illicit financial activities, an assumption that fails to account for the sophisticated operational security measures employed by contemporary terrorism financing networks that deliberately mimic legitimate transaction patterns to evade detection mechanisms.

The structural and technological constraints governing machine learning implementation in terrorism financing detection reveal systemic limitations that fundamentally compromise the theoretical efficacy of algorithmic approaches within the existing institutional framework of U.S. financial intelligence operations (Canhoto, 2021). The data accessibility constraints, particularly the inability to aggregate cross-institutional transaction data due to privacy regulations and competitive considerations, create what can be termed "institutional data silos" that provide incomplete behavioral profiles susceptible to exploitation by multi-institutional laundering schemes commonly employed in terrorism financing operations. The technological infrastructure limitations, including the inability to process unstructured data formats such as free-form text communications and voice records, systematically exclude potentially critical intelligence from algorithmic analysis, while legacy system incompatibilities create temporal and categorical blind spots in automated surveillance capabilities (Askham, 2023). These constraints are exacerbated by computational resource limitations that necessitate strategic trade-offs between concurrent analytical queries, creating temporal vulnerabilities during query transitions that sophisticated actors may exploit for operational security purposes.

The operationalization of machine learning models within terrorism financing detection frameworks demonstrates a critical divergence between theoretical algorithmic optimization and practical performance management imperatives that fundamentally alter the risk-assessment calculation of these systems. The

documented practice of parameter adjustment based on case volume management rather than intelligence-driven optimization represents what can be characterized as "performance-constrained calibration," where algorithmic sensitivity is subordinated to operational capacity limitations rather than threat detection efficacy. This operational compromise is particularly problematic in reinforcement learning applications that generate flags for unusual rather than definitively suspicious transaction patterns, creating a dependency on analyst interpretation capacity that introduces human cognitive biases and resource constraints as limiting factors in system performance. The resulting analytical framework suggests that the impact assessment of ML models in terrorism financing detection must transcend traditional performance metrics to encompass a comprehensive evaluation of their integration within the broader regulatory compliance ecosystem, institutional resource allocation mechanisms, and the dynamic threat landscape that characterizes contemporary terrorism financing methodologies, thereby requiring a reconceptualization of algorithmic efficacy within the constraints of practical counter-terrorism financing operations.

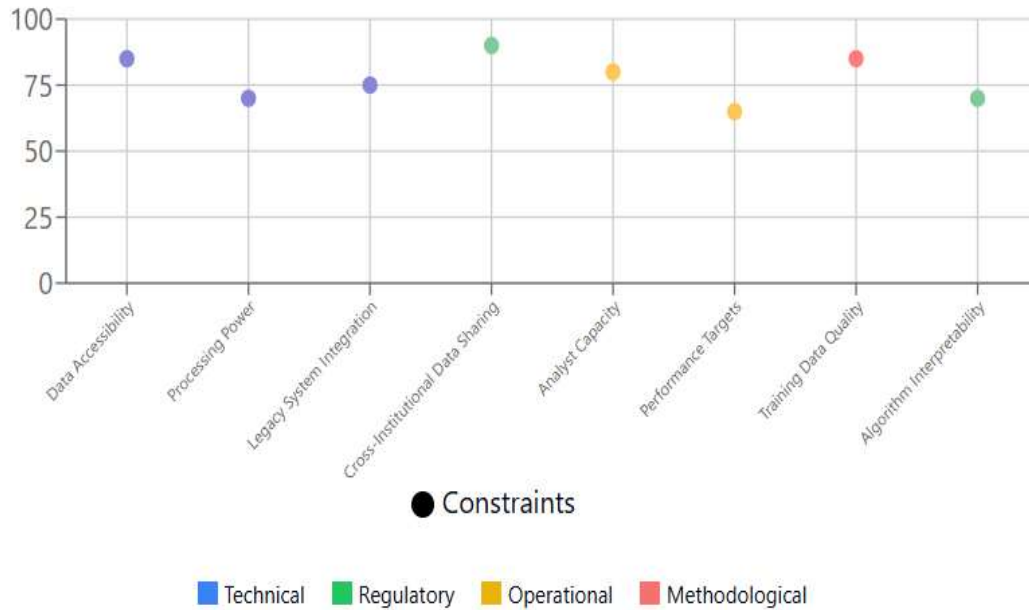
Machine Learning Performance vs. Constraints in Terrorism Financing Detection

Comprehensive Analysis of ML Model Efficacy Within U.S. Financial Industry Framework

1. ML Approach Effectiveness Matrix



2. Systematic Constraints Impact on ML Performance



3. Performance-Constrained Calibration: Theory vs. Practice Gap

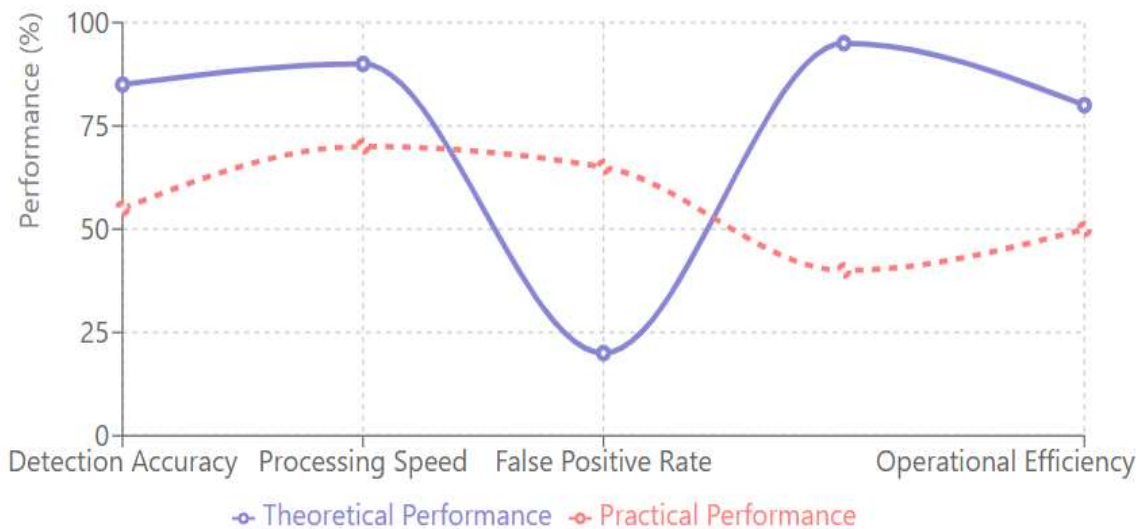


Figure 3: Machine Learning Performance vs Constraints in Terrorism Financing Detection (Raghuwanshi, 2024).

The chart above illustrates the fundamental tension between theoretical machine learning capabilities and practical implementation realities in terrorism financing detection, which revealed three key dimensions of performance degradation within financial industry frameworks. The ML Approach Effectiveness Matrix demonstrates that though supervised learning from Currency Transaction Reports (CTRs) and Suspicious

Activity Reports (SARs) achieves high data quality scores (95%), it suffers from limited data volume (15%) and modest operational efficiency (30%), while unsupervised clustering methods show inverse performance patterns with high timeliness (90%) but reduced data quality (50%). The Systematic Constraints Impact Analysis reveals that data accessibility and cross-institutional data sharing represent the most severe impediments to ML performance, with constraint severity scores exceeding 85%, followed by regulatory compliance burdens and methodological limitations that collectively create a constraining ecosystem where technical capabilities are systematically undermined by structural barriers.

Most significantly, the Performance-Constrained Calibration gap highlights the stark divergence between theoretical and practical performance across key metrics, with false positive rates exhibiting the most pronounced disparity (theoretical 20% versus practical 50%). At the same time, detection accuracy maintains relative stability, suggesting that real-world implementation forces a fundamental recalibration of ML systems that prioritizes regulatory compliance and risk aversion over optimal algorithmic performance, ultimately validating the concept that epistemological challenges, structural constraints, and operational compromises create an inherent performance ceiling that cannot be overcome through purely technical improvements.

Discussion

The theoretical proposition that machine learning algorithms can transform terrorism financing detection through sophisticated pattern recognition, multi-modal data processing and autonomous decision-making capabilities has garnered significant attention within financial industry discourse (Horobets et al. 2025). However, empirical investigation into the practical implementation of ML-based anti-terrorism financing (ATF) systems within U.S. financial institutions reveals a substantial divergence between theoretical potential and operational reality. Through a comprehensive review of related literature and empirical studies, this study demonstrates that the actual affordance of machine learning for terrorism financing detection falls considerably short of industry expectations and academic projections.

The empirical findings expose a key challenge in applying machine learning to terrorism financing detection: the phenomenon involves two separate analytical approaches that demand fundamentally different algorithms and methods. The first approach focuses on reconstructing past terrorism financing methods through descriptive profiling, which requires systematically analyzing historical transaction data, network structures and behavioral anomalies to gain a thorough understanding of terrorist financial activities. This type of descriptive modeling mainly depends on labeled datasets from confirmed terrorism financing cases, regulatory enforcement actions and intelligence reports, making supervised learning algorithms, especially ensemble methods and neural networks, suitable for recognizing patterns and capturing knowledge. The second approach centers on real-time threat detection via predictive profiling, which involves ongoing monitoring of transaction flows, behavioral changes and network shifts to catch suspicious activities early before they escalate into confirmed threats.

The findings revealed that structural constraints within U.S. financial institutions fundamentally limit their ability to fully utilize machine learning for detecting terrorism financing. This research refers to this limitation as "performance-constrained calibration." These constraints appear across several key dimensions. First, regulatory compliance requirements tend to prioritize false positive tolerance over algorithmic optimization. Second, data accessibility is restricted due to inter-agency information sharing barriers and strict privacy regulations. Third, many institutions face technological infrastructure deficiencies, which prevent real-time processing of data from multiple sources. Lastly, organizational risk

aversion often leads to a preference for interpretable, rule-based systems rather than more advanced but opaque machine learning models. Consequently, though the theoretical capability exists to develop highly sophisticated ML systems capable of identifying complex terrorism financing patterns, the practical implementation within the regulatory and operational framework of U.S. financial institutions necessitates significant compromises in algorithmic sophistication. This results in systems that operate well below their theoretical performance ceiling and often default to conservative detection thresholds that generate substantial investigative overhead while potentially missing sophisticated evasion techniques employed by contemporary terrorist networks.

Table 2: Impact of Technical and Contextual Constraints on ML Affordance Realization in Terrorism Financing Detection

Profiling Type	Intelligence Development on Terrorism Financing Patterns	Detection of Terrorism Financing Attempts
Input	<ul style="list-style-type: none"> • Historical transaction data • OFAC designation records • FinCEN SARs database • Intelligence community reports 	<ul style="list-style-type: none"> • Real-time transaction monitoring • Cross-border wire transfers • Beneficial ownership data • Sanctions screening results • Geographic risk indicators
Machine Learning Algorithm	<ul style="list-style-type: none"> • Supervised learning • Neural networks • Ensemble methods 	<ul style="list-style-type: none"> • Unsupervised clustering • Anomaly detection • Reinforcement learning • Graph analytics
Output	<ul style="list-style-type: none"> • Terrorism financing typologies • Risk assessment models • Pattern libraries • Enhanced due diligence protocols 	<ul style="list-style-type: none"> • Real-time alerts • Risk scoring • Transaction flagging • Investigation prioritization
Constraints Impacting All U.S. Financial Institutions	<ul style="list-style-type: none"> • Limited visibility into correspondent banking networks • Restricted access to classified intelligence • Privacy regulations (GLBA, state laws) • Cognitive limitations in interpreting complex ML outputs • BSA/AML regulatory requirements • Limited terrorism financing training datasets 	<ul style="list-style-type: none"> • Real-time processing limitations • Unchecked algorithmic assumptions • Inability to validate predictions against classified data • Cultural and behavioral bias in algorithms • False positive management challenges

		<ul style="list-style-type: none"> • Relevant historical case studies • Cross-agency information sharing restrictions 	
Constraints Specific to Individual Financial Institutions		<ul style="list-style-type: none"> • Legacy core banking system limitations • Incompatible data architectures • Access to proprietary terrorism financing databases • Limited analytical capacity for manual review • Resource constraints for algorithm development 	<ul style="list-style-type: none"> • Geographic service limitations • Customer demographic restrictions • Product-specific transaction patterns • Institutional risk tolerance levels • Compliance infrastructure maturity • Simultaneous monitoring system capacity

(Canhoto, 2021).

The table above systematically delineates the constraints that fundamentally limit the practical implementation of machine learning systems for terrorism financing detection within U.S. financial institutions, which reveals a complex ecosystem of technical, regulatory and operational barriers that collectively undermine the theoretical promise of ML-driven counter-terrorism finance efforts. The divergence between intelligence development and active detection profiling demonstrates that, though supervised learning algorithms can effectively process historical data sources such as OFAC designations and FinCEN Suspicious Activity Reports. This helps to develop terrorism financing typologies and risk assessment models, but the transition to real-time predictive capabilities through unsupervised clustering and reinforcement learning encounters substantially more severe constraints. Consequently, the table illustrates how the convergence of regulatory, technical and contextual constraints creates what can be termed "systemic affordance degradation," where the actual capability of ML systems to identify terrorism financing patterns operates substantially below theoretical potential. This forces financial institutions to rely on conservative, rule-based approaches that generate significant false positive rates, however, potentially missing sophisticated evasion techniques employed by contemporary terrorist networks.

Conclusion

This study set out to assess the potential of machine learning models in identifying terrorism financing patterns within the U.S. financial industry and their alignment with the objectives of the United Nations Sustainable Development Goal 16. However, machine learning offers promise in detecting anomalous transaction behaviors; our findings reveal that its impact is significantly constrained by legal, structural and organizational barriers. These include limited access to quality training data, regulatory compliance frameworks that emphasize false positive tolerance and fragmented institutional oversight that hampers inter-agency data sharing. Moreover, the complexity, opacity and high cost of implementation deter many institutions from deploying advanced AI solutions in favor of more interpretable rule-based systems. We also found no evidence of the use of advanced analytics such as sentiment analysis from online sources. At the organizational level, human judgment, risk perception and institutional readiness play significant

roles in shaping how these technologies are adopted and used. Theoretically, our research highlights the importance of understanding the technical affordances of AI and the contextual and institutional dynamics that constrain or enable their realization. Consequently, the perceived effectiveness of machine learning in counterterrorism finance remains overstated in practice and its true potential can only be unlocked through coordinated national-level frameworks, improved access to labeled data and stronger collaboration between regulatory bodies and financial institutions. Future research should explore these dimensions further to enhance the responsible deployment of AI in national security contexts.

Reference

1. Askham, G. R. (2023). A practice-led investigation into the role of play as a feedback mechanism between the human and technological systems-as revealed through art & technology projects (Doctoral dissertation, London Metropolitan University).
2. Azzahra, A. (2025). Examining the Role of Financial Intelligence in Preventing, Disrupting, and Reducing Child Sex Trafficking.
3. Broad, R., Lord, N., & Duncan, C. (2022). The financial aspects of human trafficking: A financial assessment framework. *Criminology & Criminal Justice*, 22(4), 581-600.
4. Brooks, A., Carter, S., & Idowu, M. (2025). AI-Powered Defense Strategies: Enhancing Cybersecurity and Combating Terrorism Financing in the US Financial Sector.
5. Brown, R. (2017). *The Chinese and Indian corporate economies: a comparative history of their search for economic renaissance and globalization*. Routledge.
6. 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.
7. 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.
8. 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.
9. Carpentier, C. L., & Braun, H. (2020). Agenda 2030 for Sustainable Development: A powerful global framework. *Journal of the International Council for Small Business*, 1(1), 14-23.
10. Gheisari, M., Wang, G., & Bhuiyan, M. Z. A. (2017, July). A survey on deep learning in big data. In 2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC) (Vol. 2, pp. 173-180). IEEE.
11. Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*.
12. Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*.
13. Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*.
14. Jackson, B. A., Rhoades, A. L., Reimer, J. R., Lander, N., Costello, K., & Beaghley, S. (2019). *Practical Terrorism Prevention*. RAND Corporation.

15. Kumar, D., & Singh, S. (2024). Analyzing the impact of machine learning algorithms on risk management and fraud detection in financial institutions. *International Journal of Research Publication and Reviews*, 5(5), 1797-1804.
16. Leal Filho, W., Tripathi, S. K., Andrade Guerra, J. B. S. O. D., Giné-Garriga, R., Orlovic Lovren, V., & Willats, J. (2019). Using the sustainable development goals towards a better understanding of sustainability challenges. *International Journal of Sustainable Development & World Ecology*, 26(2), 179-190.
17. Leonardi, P. M. (2013). When does technology use enable network change in organizations? A comparative study of feature use and shared affordances. *MIS quarterly*, 749-775.
18. Mbiva, S. M., & Correa, F. M. (2024). Machine Learning to Enhance the Detection of Terrorist Financing and Suspicious Transactions in Migrant Remittances. *Journal of Risk and Financial Management*, 17(5), 181.
19. Mekpor, E. S. (2019). Anti-money laundering and combating the financing of terrorism compliance: Are FATF member states just scratching the surface?. *Journal of Money Laundering Control*, 22(3), 451-471.
20. Montasari, R. (2024). Machine learning and deep learning techniques in countering cyberterrorism. In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses* (pp. 135-158). Cham: Springer International Publishing.
21. Nwoke, J. (2024). Digital Transformation in Financial Services and FinTech: Trends, Innovations and Emerging Technologies. *International Journal of Finance*, 9(6), 1-24.
22. Parker, M. (2014). Cicero, money and the challenge of 'new terrorism': is counter terrorist financing (CTF) a critical inhibitor? Should the emphasis on finance interventions prevail? (Doctoral dissertation, University of St Andrews).
23. Raghuwanshi, P. (2024). DEEP LEARNING MODEL FOR DETECTING TERROR FINANCING PATTERNS IN FINANCIAL TRANSACTIONS. *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (online), 3(3), 288-296.
24. Shehzadi, T. (2024). Reinforcement Learning-Based Autonomous Systems for Cyber Threat Detection and Response. *Eastern European Journal for Multidisciplinary Research*, 1(1), 123-137.
25. Volkoff, O., & Strong, D. M. (2017). Affordance theory and how to use it in IS research. In *The Routledge companion to management information systems* (pp. 232-245). Routledge.
26. Westgard, J. O., & Westgard, S. A. (2016). Quality control review: implementing a scientifically based quality control system. *Annals of clinical biochemistry*, 53(1), 32-50.
27. Zoli, C., Steinberg, L. J., Grabowski, M., & Hermann, M. (2018). Terrorist critical infrastructures, organizational capacity and security risk. *Safety science*, 110, 121-130.