World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Strengthening U.S. financial industry defenses against terrorism financing: A machine learning to anti-money laundering systems

Omogbolahan Alli [1,*], Chinedu Mbabie [2], Okechukwu Eze Chigbu [3], Karl Kiam [4] and Ajibola Olapade [2]

[1] *Hult International Business School, Boston, Massachusetts, USA.*
[2] *Department of Computer Science, University of Lagos, Akoka, Lagos Nigeria.*
[3] *College of Business, University of Louisville, Kentucky USA.*
[4] *Data Science and Analytics Institute, University of Oklahoma, Norman USA.*

World Journal of Advanced Engineering Technology and Sciences, 2023, 10(02), 385-393

Publication history: Received on 08 September 2023; revised on 15 December 2023; accepted on 18 December 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.10.2.0275

Abstract

Terrorism financing remains a severe threat to the stability of the U.S. financial system, necessitating continuous advancements in anti-money laundering (AML) strategies. This paper explores the integration of machine learning (ML) into AML systems to enhance the detection and prevention of illicit financial activities linked to terrorism financing. While ML-driven AML solutions offer improved accuracy and adaptability, they also present challenges, such as regulatory compliance, model explainability, adversarial attacks, and data privacy concerns. The paper examines the risks posed by adversarial ML tactics, where criminals manipulate transaction patterns to evade detection, and highlights the ethical concerns surrounding biased AML models that may disproportionately target specific demographics. Furthermore, the paper underscores the need for explainable AI (XAI) to ensure regulatory transparency and proposes the adoption of federated learning to enhance data privacy without compromising detection capabilities. Ultimately, this research advocates for a balanced approach that strengthens financial defenses against terrorism financing while ensuring compliance, fairness, and privacy protection in ML-driven AML systems.

Keywords: Terrorism Financing; Anti-Money Laundering; Machine Learning; Financial Crime; Adversarial ML; Explainable AI; Federated Learning

1. Introduction

Terrorism financing remains a threat to global security and financial stability, enabling extremist organizations to sustain operations, recruit members, and orchestrate attacks. The United Nations estimates that between $800 billion and $2 trillion is laundered annually, representing 2-5% of global GDP, yet authorities detect only a small fraction of these illicit transactions (1). In the United States, financial institutions face mounting challenges in preventing terrorism financing, as criminals increasingly exploit regulatory loopholes and technological vulnerabilities to evade detection (2). Recent enforcement actions, such as the guilty pleas and $30 million in combined fines involving the co-founders of BitMEX in 2022, underscore the weaknesses in existing financial surveillance mechanisms, particularly in detecting complex money laundering patterns linked to terrorism. BitMEX was found to have willfully violated the Bank Secrecy Act by failing to implement adequate anti-money laundering (AML) controls, allowing illicit actors to transact anonymously and facilitating money laundering activities (3). These challenges necessitate a more adaptive and intelligence-driven approach to counteract financial crimes effectively.

Traditional AML frameworks have long served as the first line of defense against illicit financial activities, requiring financial institutions to monitor transactions and report suspicious activities. However, the rapid evolution of financial

* Corresponding author: Omogbolahan Alli

crime tactics, especially in digital finance and cryptocurrency markets, has exposed limitations in conventional AML measures. Manual transaction monitoring and rule-based systems often struggle to identify sophisticated money laundering schemes that involve layering, structuring, and the use of anonymized digital assets. As a result, there is a growing need for more advanced AML mechanisms, such as machine learning and artificial intelligence, to enhance financial surveillance and improve the detection of terrorism financing risks (4).

Machine learning has emerged as a transformative tool in financial security, offering enhanced detection capabilities through advanced pattern recognition, anomaly detection, and predictive analytics. Unlike static rule-based systems, machine learning models continuously learn from financial data, identifying new laundering methods and adapting to changing threat landscapes (5). Its application in AML has improved financial crime detection, with institutions implementing AI-driven solutions reporting fewer undetected suspicious activities, greater operational efficiency, and reduced false positives, allowing compliance teams to focus on high-risk cases. Regulators such as the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) increasingly advocate for AI-driven compliance mechanisms to enhance the accuracy of suspicious activity reporting. However, challenges such as privacy concerns, algorithmic biases, and regulatory constraints must be addressed to ensure transparency, accountability, and compliance with legal frameworks.

This study explores the role of machine learning in strengthening AML systems against terrorism financing, examining its effectiveness in enhancing financial security while considering its ethical and regulatory implications. By analyzing both theoretical and practical dimensions of AI-driven AML solutions, this research aims to contribute to a deeper understanding of how machine learning can be leveraged to combat terrorism financing in the U.S. financial industry. Given the evolving nature of financial crimes, a comprehensive assessment of these technologies is necessary to inform future policy directions and ensure a balanced approach to security, privacy, and regulatory oversight.

2. Conceptual Analysis of Terrorism Financing, Money Laundering and Anti-Money Laundering

2.1. Defining Terrorism Financing: Methods and Networks

Terrorism financing is a sophisticated process involving the collection, movement, and distribution of financial resources to support terrorist activities (6). Unlike conventional financial crimes that focus on personal gain, terrorism financing prioritizes secrecy, efficiency, and sustainability. The methods used in terrorism financing vary, with some relying on traditional criminal enterprises, while others exploit legal structures. Common sources of terrorist funding include drug trafficking, arms smuggling, kidnapping for ransom, illicit trade, fraud, and cybercrime. However, terrorist groups also capitalize on legitimate means such as charities, business investments, and crowdfunding campaigns to evade scrutiny (7).

Terrorist financing networks are often highly decentralized, making them difficult to detect and disrupt. These networks span multiple countries and involve a mix of formal and informal financial systems. Hawala networks, a traditional form of informal value transfer, remain a preferred method for transferring funds across borders due to their anonymity and lack of documentation (8). Additionally, the rise of cryptocurrencies has introduced a new dimension to terrorism financing, allowing for peer-to-peer transactions that bypass traditional banking channels (9).

The vulnerabilities in financial systems stem from gaps in regulatory enforcement, reliance on outdated detection mechanisms, and the adaptability of terrorist groups. While large financial institutions have strengthened their compliance measures, smaller banks, money service businesses, and fintech companies often lack the resources or expertise to detect sophisticated terrorism financing schemes. Moreover, the use of shell companies and anonymous corporate structures allows terrorist financiers to obscure their identities, further complicating law enforcement efforts.

2.2. Money Laundering in Terrorism Financing

Money laundering plays an integral role in terrorism financing, as it enables the movement and concealment of funds while reducing the risk of detection (10). The process of laundering money typically involves three stages: placement, layering, and integration (11).

- Placement – Illicit funds are introduced into the financial system, often through cash deposits, trade-based transactions, or real estate investments. Terrorist organizations frequently receive funding through charities or personal remittances, making placement less conspicuous.

- Layering – Transactions are structured to obscure the origin of funds. This may involve moving money across multiple accounts, engaging in currency exchanges, or conducting transactions through shell companies. The Panama Papers leaks exposed how offshore financial structures have been used to launder illicit funds, including those tied to terrorism financing.
- Integration – Once laundered, the funds are reinvested into the economy through seemingly legitimate means, such as business operations, asset purchases, or investments in financial markets.

Unlike traditional money laundering, where criminals seek to enjoy illicit wealth, terrorism financing often follows a reverse laundering model in which legally acquired funds are intentionally directed toward illicit activities. This fundamental difference complicates detection efforts, as small-value transactions, cash-based donations, and alternative remittance systems may not trigger conventional AML red flags. As terrorist financiers frequently operate within legal frameworks, merely monitoring transactions is insufficient. Instead, AML systems must incorporate behavioral analysis and network-based approaches to uncover hidden patterns and connections. To enhance detection and mitigation efforts, financial institutions have increasingly adopted the Risk-Based Approach (RBA), which prioritizes resources based on the level of risk associated with customers, transactions, and jurisdictions (12). This strategy has proven effective in identifying high-risk geographies, industries, and customer profiles that could be exploited for terrorism financing, ultimately strengthening financial security and compliance frameworks

2.3. The Evolution and Types of AML Systems in the US Financial Industry

The US financial industry has undergone several AML reforms over the past five decades in response to emerging financial crimes. The Bank Secrecy Act (BSA) of 1970, officially known as the Currency and Foreign Transactions Reporting Act, was the first major legislative framework aimed at combating money laundering by requiring financial institutions to maintain records and report suspicious transactions. However, it was the USA PATRIOT Act (2001) that transformed AML enforcement following the 9/11 attacks, introducing stricter customer due diligence (CDD), information-sharing protocols, and transaction monitoring obligations to prevent terrorism financing (13). Despite these regulations, traditional AML systems have struggled with false positives, inefficient compliance processes, and an inability to adapt to evolving threats. To address these shortcomings, financial institutions are increasingly integrating ML and AI into AML frameworks.

2.4. Types of AML Systems in the US Financial Industry

- **Rule-Based AML Systems** – Traditional AML frameworks rely on pre-defined rules to flag suspicious transactions, such as large cash deposits or rapid fund transfers to high-risk countries (14). While useful, these systems often fail to detect complex money laundering structures.
- **Behavioral Analytics and Pattern Recognition** – Modern AML systems leverage big data analytics and network modeling to identify deviations from normal transaction behaviors (15). By analyzing past financial activities, these systems can detect anomalous transactions that indicate potential laundering or terrorism financing.
- **Machine Learning-Powered AML Systems** – Leading financial institutions are now deploying ML-driven AML models that use natural language processing (NLP), anomaly detection algorithms, and predictive analytics to improve detection accuracy (16). A prominent example is JP Morgan Chase's AI-driven AML system, which uses network analysis and behavioral profiling to uncover hidden money laundering patterns. This system has reduced false positives while improving regulatory compliance.
- **Cryptocurrency AML Solutions** – With the rise of digital assets, US regulators have mandated the implementation of blockchain analytics and transaction monitoring tools to track illicit crypto transactions (17). The FinCEN has introduced stricter KYC and AML rules for cryptocurrency exchanges to prevent terrorism financing through digital currencies.

The evolution of AML systems reflects the growing complexity of financial crimes and the need for adaptive, technology-driven solutions. As financial criminals exploit new technologies such as decentralized finance (DeFi) and privacy coins, the effectiveness of AML enforcement will depend on the ability of regulators, financial institutions, and technology providers to collaborate in strengthening financial security measures. The future of AML will likely involve AI-powered predictive risk assessment, biometric verification, and real-time transaction monitoring, ensuring a more proactive and intelligence-driven approach to countering terrorism financing.

3. Traditional Aml Systems and Their Limitations

The United States' AML framework has long relied on traditional compliance-based mechanisms to detect and prevent financial crimes, including terrorism financing. These systems are primarily designed to identify suspicious activities,

enforce regulatory compliance, and mitigate financial risks within institutions. However, the increasing sophistication of financial crime networks, coupled with the limitations of rule-based detection models, has led to inefficiencies, regulatory failures, and the inability to proactively combat terrorism financing. The shortcomings of traditional AML mechanisms have necessitated the integration of advanced technologies such as ML to enhance threat detection and mitigation. This section examines the core traditional AML systems, their limitations, demonstrating the need for a more intelligent and adaptive AML framework.

3.1. Rule-Based Transaction Monitoring and Suspicious Activity Reports (SARs)

One of the cornerstones of traditional AML systems is rule-based transaction monitoring, which involves predefined thresholds and red flags to identify potentially illicit transactions. Financial institutions are required to monitor and flag transactions that exceed certain limits, display irregular patterns, or originate from high-risk jurisdictions. When a transaction meets these criteria, a Suspicious Activity Report (SAR) is generated and submitted to regulatory agencies for further investigation (14). Despite its widespread use, rule-based monitoring is inherently static, reactive, and prone to false positives:

- **Over-Reliance on Predefined Rules**: Criminals **structure transactions** just below reporting thresholds to evade detection (e.g., "smurfing," where funds are broken into small amounts below the $10,000 reporting limit) (18).
- **High False Positive Rates**: Up to 90% of flagged transactions in traditional AML systems result in false positives, leading to wasted resources and inefficient investigations (19).
- **Failure to Detect Emerging Threats**: Rule-based systems struggle to identify new and evolving laundering methods, as they only detect known patterns rather than emerging tactics.

3.2. Know Your Customer (KYC) and Customer Due Diligence (CDD) Practices

KYC and CDD are regulatory requirements that mandate financial institutions to verify customer identities, assess risk profiles, and monitor ongoing account activities. These measures are critical in preventing financial institutions from being used as conduits for terrorism financing and other illicit activities. However, traditional KYC/CDD processes remain heavily manual, compliance-driven, and often ineffective against sophisticated crime networks (20). Notable limitations include:

- **Identity Fraud and Document Manipulation**: Criminals exploit loopholes in identity verification systems, using fake documents, stolen credentials, and shell companies to create legitimate-looking financial profiles.
- **Regulatory Arbitrage**: Terror financiers **exploit gaps between different regulatory regimes**, setting up accounts in **jurisdictions with weaker AML requirements**.
- **Limited Cross-Border Visibility**: Traditional KYC/CDD frameworks **struggle to track financial activities across multiple jurisdictions**, allowing criminals to **move funds undetected** through international networks.

3.3. Compliance-Based AML Frameworks and Manual Investigations

Traditional AML enforcement relies heavily on manual audits, regulatory compliance reporting, and case-by-case investigations. Financial institutions are required to submit reports, conduct internal audits, and comply with a growing list of AML regulations. However, this approach focuses on fulfilling regulatory obligations rather than proactively identifying criminal networks (21). Key limitations **include:**

- **Reactive Instead of Proactive**: Investigations typically occur **after crimes have already been committed**, rather than detecting threats in real time.
- **Regulatory Overload**: Financial institutions spend billions annually on **compliance efforts**, yet regulatory bodies still issue **massive fines for AML failures**.
- **Failure to Track Complex Money Laundering Networks**: Criminals use **layering techniques** (moving funds through multiple transactions and intermediaries) to obscure their activities, **defeating traditional compliance models**.

4. Machine Learning In Anti-Money Laundering Systems

Terrorism financing remains a pressing global threat, exploiting weaknesses in financial systems to launder illicit funds for extremist operations. Traditional AML mechanisms, rule-based transaction monitoring, KYC, CDD, and SARs, have proven inadequate in detecting and disrupting the sophisticated financial networks used by terrorist organizations. These conventional approaches rely on predefined rules and historical patterns, making them rigid, prone to false

positives, and ineffective against evolving tactics. ML provides a transformative data-driven approach, offering adaptability, automation, and enhanced detection capabilities that significantly strengthen AML measures against terrorism financing.

By integrating supervised and unsupervised learning, NLP, network analysis, deep learning, federated learning, and reinforcement learning, financial institutions can overcome traditional AML limitations, reduce false positives, enhance real-time risk assessment, and improve cross-border intelligence sharing.

4.1. Enhancing Anomaly Detection: Overcoming Rule-Based Transaction Monitoring Limitations

Traditional AML systems primarily rely on rule-based transaction monitoring, where predefined thresholds trigger alerts for suspicious activity. However, terrorist financiers and money launderers have become adept at circumventing these static rules by structuring transactions just below reporting thresholds (smurfing) or disguising illicit flows through shell companies and digital assets (18). This rigidity leads to high false positives, overwhelming compliance teams with unnecessary investigations while failing to detect subtler, sophisticated laundering techniques.

Machine learning significantly improves anomaly detection by leveraging supervised and unsupervised learning to identify deviations from expected transaction behaviors rather than relying on fixed rules (22). Supervised learning models, trained on historical money laundering cases, can recognize patterns indicative of terrorism financing, such as frequent small-value international transfers to high-risk regions or round-tripping schemes involving cryptocurrency exchanges. For instance, financial institutions utilizing Random Forest and Gradient Boosting algorithms have reported 30% improvement in identifying structured layering schemes used to finance terrorism (23).

Unsupervised learning, particularly clustering algorithms like K-Means and Isolation Forests, detects previously unknown laundering strategies by grouping transactions that exhibit statistical anomalies. This is especially useful in early-stage terrorism financing, where transactions might not yet resemble known typologies but still deviate from a customer's expected behavior (24).

4.2. Advancing Transaction Narrative Analysis: Overcoming SARs and Human-Led Reviews

Another major limitation of traditional AML systems is their reliance on manual transaction reviews and SARs, which are often time-consuming, inconsistent, and reactive rather than proactive. Financial criminals frequently manipulate transaction descriptions, using vague terms or coded language to avoid detection. Compliance teams struggle to analyze large volumes of SARs, leading to delayed responses and missed opportunities to intercept terrorism financing flows.

NLP directly addresses this weakness by automating the extraction and analysis of transaction narratives. Instead of relying on compliance officers to manually inspect descriptions, NLP models can detect suspicious keywords, phrases, and hidden patterns indicative of terrorism financing (25). By contextualizing transaction data, NLP reduces false positives by distinguishing benign transactions (e.g., frequent remittances for family support) from truly suspicious transfers (e.g., multiple small-value donations to high-risk NGOs with no operational transparency). This enables faster, more accurate identification of illicit funds before they are successfully laundered.

4.3. Uncovering Hidden Networks: Overcoming Limitations of Isolated Transaction Monitoring

Traditional AML systems focus on individual transactions, making them ineffective in detecting complex, multi-layered financial networks that terrorist groups use to move funds across borders. Many laundering schemes involve multiple intermediaries, shell companies, and offshore accounts, making it nearly impossible for rule-based systems to connect disparate suspicious transactions.

Network analysis and Graph Neural Networks (GNNs) revolutionize AML by mapping transactional relationships across multiple entities, exposing hidden connections between individuals, businesses, and criminal organizations. Rather than treating each transaction as an isolated event, ML-driven graph analytics reveal underlying money laundering structures, helping authorities dismantle entire financing networks (26).

4.4. Deep Learning and Pattern Recognition: Reducing False Positives in AML

A notable issue in traditional AML compliance is high false positives, where legitimate transactions are frequently flagged, creating inefficiencies and compliance bottlenecks. This is particularly problematic in charitable donations, cryptocurrency transactions, and international remittances, which are often mistakenly classified as suspicious due to their high-risk nature.

Deep learning models, particularly Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, offer enhanced pattern recognition, identifying sophisticated money laundering sequences while filtering out benign activities (27).

4.5. Federated Learning: Overcoming Cross-Border Data-Sharing Barriers

One of the biggest challenges in global AML enforcement is the inability to share sensitive financial data across jurisdictions due to privacy laws. This restriction hampers intelligence-sharing efforts, allowing terrorist financiers to exploit regulatory blind spots. Federated learning (FL) presents a privacy-preserving solution, enabling multiple financial institutions to collaborate on AML models without directly sharing raw data (28). By training ML models on decentralized datasets, FL allows banks to collectively enhance their detection capabilities while complying with data protection laws.

5. Challenges and Ethical Considerations in Using Machine Learning for Aml

While ML has revolutionized AML and CTF efforts by enhancing anomaly detection, automating transaction analysis, and uncovering hidden financial networks, its deployment comes with challenges and ethical considerations. The reliance on large datasets, algorithmic decision-making and real-time transaction monitoring raises critical concerns related to data privacy, bias, adversarial machine learning, and regulatory compliance. These issues not only affect the efficiency of AML frameworks but also pose legal, ethical, and operational risks that financial institutions and regulators must carefully navigate.

5.1. Data Privacy and Protection Concerns: Balancing Surveillance with Confidentiality

One of the most pressing challenges in ML-driven AML is the need for vast amounts of financial transaction data to train models effectively. Financial institutions and regulators require sensitive customer information, including account activity, geolocation data, transaction histories, and communication records, to build predictive models. However, this raises several privacy concerns, particularly in jurisdictions with stringent data protection laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

ML exacerbates these risks by requiring continuous access to financial data for model training and refinement, potentially conflicting with legal data minimization and retention policies (29). To address this challenge, federated learning has emerged as a privacy-preserving alternative. This approach allows financial institutions to train ML models on decentralized data sources without directly sharing sensitive information. Research has demonstrated federated learning's effectiveness in enhancing AML detection while ensuring compliance with data protection laws (28).

5.2. Bias and Fairness in AI-Driven Financial Surveillance

Bias in ML-driven AML models presents ethical and regulatory challenges, particularly when historical data reflects discriminatory patterns in financial surveillance. Machine learning algorithms trained on biased datasets can disproportionately flag transactions from certain demographics, nationalities, or industries as high-risk, leading to unfair treatment of legitimate customers. This not only undermines trust in financial institutions but also raises concerns about compliance with anti-discrimination laws and ethical AI practices (30).

To mitigate bias, financial institutions must adopt fairness-aware ML techniques, such as re-weighting algorithms that correct historical imbalances and adversarial debiasing methods that reduce discriminatory patterns in transaction monitoring. Regular audits and impact assessments should be conducted to identify and rectify potential biases in AML models. Additionally, the development of more inclusive and diverse datasets that incorporate global transaction patterns, rather than over-relying on Western banking norms, can help reduce unintended discrimination.

5.3. The Risk of Adversarial Machine Learning and Evasion Tactics by Criminals

Adversarial machine learning presents a challenge in the financial sector, as criminals continually adapt to evade detection by manipulating machine learning models used in AML efforts. This involves exploiting vulnerabilities in AI systems to bypass financial surveillance mechanisms. For instance, North Korean hackers have been implicated in sophisticated cyberattacks aimed at financial institutions, including the theft of cryptocurrency to fund illicit activities (31). Common evasion tactics employed by such factors include transaction obfuscation, adaptive structuring, and synthetic identity fraud. To counter these adversarial attacks, financial institutions are encouraged to integrate defensive machine learning techniques.

5.4. Regulatory Compliance and Explainability of ML Models

The integration of ML in AML efforts has introduced challenges related to the explainability of AI-driven decisions. Many ML models, especially those based on deep learning, function as 'black boxes,' making it difficult to interpret their decision-making processes. This opacity poses compliance issues, as financial institutions are required to justify why specific transactions are flagged as suspicious (32).

To address these challenges, financial institutions are encouraged to adopt Explainable AI (XAI) techniques. These methods aim to break down ML model decisions into human-readable formats, facilitating regulatory compliance and enhancing trust. Techniques such as decision trees, SHAP (SHapley Additive exPlanations) values, and LIME (Local Interpretable Model-agnostic Explanations) can be employed to elucidate which transaction features trigger AML alerts. Furthermore, establishing robust model validation and governance frameworks, including periodic third-party audits, is essential to maintain compliance and ensure the reliability of AI-driven AML systems.

By prioritizing explainability in ML-driven AML systems, financial institutions can better meet regulatory expectations, reduce the risk of compliance violations, and enhance the overall effectiveness of their financial crime detection efforts.

6. Conclusion and Recommendations

Traditional AML methods, including rule-based transaction monitoring, KYC protocols, and SARs, have proven inadequate in addressing the complexities of modern financial crimes. These frameworks struggle with high false positives, inefficiencies in detecting sophisticated networks, and vulnerability to evolving laundering techniques. ML offers a transformative approach by leveraging adaptive algorithms, anomaly detection, and network analysis to enhance AML efforts and counter terrorism financing. However, integrating ML into AML strategies presents challenges, including data privacy concerns, regulatory compliance, and the risk of adversarial manipulation.

To modernize AML frameworks, regulatory bodies must establish AI-compliant guidelines that ensure transparency and explainability in ML-driven financial surveillance. Institutions should adopt risk-based AI compliance models, encourage regulatory sandboxes for AI experimentation, and develop standardized ML-based AML solutions. The UK's Joint Money Laundering Intelligence Taskforce (JMLIT) and Singapore's Monetary Authority (MAS) Veritas Initiative serve as examples of successful AI regulatory integration, enhancing intelligence-sharing and model transparency.

Strengthening public-private partnerships is crucial for intelligence sharing and fraud detection. Financial institutions should collaborate with regulatory agencies to enhance real-time ML-driven suspicious transaction reports, fostering secure data-sharing alliances. The success of AI-driven AML collaboration, as seen in the UK's National Crime Agency's exposure of a £250 million laundering scheme, demonstrates the potential of collective AI-powered financial surveillance. Similarly, improving cross-border cooperation is vital, as financial crime networks exploit jurisdictional gaps. A unified global AI-driven AML framework, as advocated by FATF, would improve cross-border transaction monitoring and prevent terrorism financing through real-time anomaly detection.

Standardizing AI-driven AML solutions across financial institutions will enhance detection efficiency while ensuring regulatory alignment. Adopting open-source AI models and industry-wide data structuring standards, such as ISO 20022, will facilitate interoperability. Additionally, ethical AI deployment remains essential in preventing algorithmic bias, ensuring privacy compliance, and maintaining the explainability of financial crime detection models. The European Banking Authority's AI Ethics Initiative underscores the importance of balancing financial security with responsible AI use.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] United Nations. Tax abuse, money laundering and corruption plague global finance | Nações Unidas. Available from: https://www.un.org/pt/desa/tax-abuse-money-laundering-and-corruption-plague-global-finance

[2] U.S. Department of the Treasury. National Strategy for Combating Terrorist and Other Illicit Financing. 2022. Available from: https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf.

[3] Cohen L, Godoy J, Cohen L, Godoy J. Founders of crypto exchange BitMEX plead guilty to bank secrecy act violations. Reuters. 2022 Feb 24. Available from: https://www.reuters.com/technology/founders-crypto-exchange-bitmex-plead-guilty-bank-secrecy-act-violations-2022-02-24/

[4] Financial Action Task Force. Opportunities and Challenges of New Technologies for AML/CFT. Paris: FATF; 2021. Available from: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.

[5] Yussuf MF, Oladokun P, Williams M. Enhancing Cybersecurity Risk Assessment in Digital Finance Through Advanced Machine Learning Algorithms. Int J Comput Appl Technol Res. 2020;9(6):217-235. Available from: https://ijcat.com/archieve/volume9/issue6/ijcatr09061005.pdf.

[6] Teichmann FM. Current trends in terrorist financing. J Financ Regul Compliance. 2022 Jan 13;30(1):107–25.

[7] Freeman M, Ruehsen M. Terrorism Financing Methods: An Overview. Perspectives on Terrorism. 2013;7(4). Available from: https://pt.icct.nl/article/terrorism-financing-methods-overview.

[8] The Hawala System: A Risky Alternative to Traditional Banking. ACAMS Today. 2023 Mar 10. Available from: https://www.acamstoday.org/the-hawala-system-a-risky-alternative-to-traditional-banking/

[9] Akartuna EA, Johnson SD, Thornton AE. The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. Secur J. 2023 Dec;36(4):615–50.

[10] Canhoto AI. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. J Bus Res. 2021 Jul;131:441–52.

[11] Calafos MW, Dimitoglou G. Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency. In: Daimi K, Dionysiou I, El Madhoun N, editors. Principles and Practice of Blockchains. Cham: Springer International Publishing; 2023. p. 271–300. Available from: https://link.springer.com/10.1007/978-3-031-10507-4_12

[12] Jensen R, Iosifidis A. Fighting Money Laundering with Statistics and Machine Learning. arXiv; 2022. Available from: https://arxiv.org/abs/2201.04207

[13] Keyani C. Lawfare and US Economic Supremacy: The Bank Secrecy Act, FCPA, USA PATRIOT Act, and OFAC Sanctions. Ohio N Univ Int Law J. 2023;1(1):3. Available from: https://digitalcommons.onu.edu/ilj/vol1/iss1/3.

[14] Ketenci UG, Kurt T, Önal S, Erbil C, Aktürkoğlu S, İlhan HŞ. A Time-Frequency based Suspicious Activity Detection for Anti-Money Laundering. arXiv; 2020. Available from: https://arxiv.org/abs/2011.08492

[15] Krishnapriya G, Prabakaran M. Money laundering analysis based on time variant behavioral transaction patterns using data mining. J Theor Appl Inf Technol. 2014 Sep 10;67(1):12-17. Available from: https://www.jatit.org/volumes/Vol67No1/2Vol67No1.pdf.

[16] Cardoso M, Saleiro P, Bizarro P. LaundroGraph: Self-Supervised Graph Representation Learning for Anti-Money Laundering. arXiv; 2022. Available from: https://arxiv.org/abs/2210.14360

[17] Kirkpatrick K, Stephens A, Gerber J, Nettesheim M, Bellm S. Understanding regulatory trends: digital assets & anti-money laundering. J Invest Compliance. 2021 Oct 28;22(4):345–53.

[18] Baranello AM. Money Laundering and the Art Market: Closing the Regulatory Gap. Seton Hall Legislative Journal. 2021;45(3):695-737. Available from: https://scholarship.shu.edu/shlj/vol45/iss3/6/.

[19] Chen Z, Van Khoa LD, Teoh EN, Nazir A, Karuppiah EK, Lam KS. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowl Inf Syst. 2018 Nov;57(2):245–85.

[20] Shust PM, Dostov V. Implementing innovative customer due diligence: proposal for universal model. J Money Laund Control. 2020 Mar 25;23(4):871–84.

[21] Zavoli I, King C. The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis. Mod Law Rev. 2021 Jul;84(4):740–71.

[22] Usmani UA, Happonen A, Watada J. A Review of Unsupervised Machine Learning Frameworks for Anomaly Detection in Industrial Applications. In: Arai K, editor. Intelligent Computing. Cham: Springer International Publishing; 2022. p. 158–89. (Lecture Notes in Networks and Systems; vol. 507). Available from: https://link.springer.com/10.1007/978-3-031-10464-0_11

[23] Vassallo D, Vella V, Ellul J. Application of Gradient Boosting Algorithms for Anti-money Laundering in Cryptocurrencies. SN Comput Sci. 2021 May;2(3):143.

[24] Krikorian M. Fraud Detection Applying Unsupervised Learning Techniques. Medium. 2021 Jun 29. Available from: https://medium.com/southworks/fraud-detection-applying-unsupervised-learning-techniques-4ae6f71b266f.

[25] Pavlidis G. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. J Money Laund Control. 2023 Dec 18;26(7):155–66.

[26] Nicholls J, Kuppa A, Le-Khac NA. Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access. 2021;9:163965–86.

[27] Alghofaili Y, Albattah A, Rassam MA. A Financial Fraud Detection Model Based on LSTM Deep Learning Technique. J Appl Secur Res. 2020 Oct 1;15(4):498–516.

[28] Zhang H, Hong J, Dong F, Drew S, Xue L, Zhou J. A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection. arXiv; 2023. Available from: https://arxiv.org/abs/2302.03654

[29] Sun PJ. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. IEEE Access. 2019;7:147420–52.

[30] Akter S, Dwivedi YK, Biswas K, Michael K, Bandara RJ, Sajib S. Addressing Algorithmic Bias in AI-Driven Customer Management: J Glob Inf Manag. 2021 Aug 23;29(6):1–27.

[31] Office of Public Affairs | Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe | United States Department of Justice. 2021. Available from: https://www.justice.gov/archives/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

[32] Bibal A, Lognoul M, De Streel A, Frénay B. Legal requirements on explainability in machine learning. Artif Intell Law. 2021 Jun;29(2):149–69.