International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

AI-Powered Financial Forensics in Automating Anomaly Detection and AML Compliance

Geol Gladson Battu

Abstract: ***Financial transactions have become more complex and faster than ever before and have put the traditional Anti-Money Laundering and forensic accounting processes under strain. The financial industry faces mounting pressure to detect and prevent fraudulent activities, money laundering, and regulatory breaches with increasing speed and accuracy. Rules based approaches frequently do not scale to the complexity and volume of transactions experienced within the financial services industry. This paper explores how AI and ML can be integrated into financial forensics especially automating anomaly detection and AML compliance. A spectrum of AI models, including supervised, unsupervised, and reinforcement learning methods, are analyzed to ascertain their level of efficacy for the purpose of detecting complex hidden patterns that might signal illegitimate activities. This paper explores real-world use cases in which AI systems outperform the manual and static rule-based systems in finding anomalies with very low false positive rates. Additionally, the paper explores the growing need for explainable AI models, data privacy and shifting compliance requirements. Further, the paper outlines how AI-enabled financial forensics not only improves the ability to detect anomalies but improves the efficiency of the compliance process, decreases the cost of operations, and offers measures to respond to various complex financial crimes. This study underscores AI as the central driver of disruptive innovation towards financial surveillance and regulatory compliance.***

Keywords: Artificial Intelligence, Financial Forensics, Anomaly Detection, Anti-Money Laundering, Compliance Automation, Machine Learning

1.Introduction

As transaction volumes, complexity and cross-border activities are increasing, rule-based Anti-Money Laundering systems and manual forensics are finding it harder to cope. These traditional approaches generally suffer from high false positive rates, inflexible rule configuration and trouble adapting to new threat patterns [1]. Artificial Intelligence (AI) presents a new way forward for the field of financial forensics. It offers an opportunity to automate anomaly detection and helps with present intelligence AML compliance efforts across completely new domains. With the help of machine learning, natural language processing (NLP) and time-series anomaly detection models, financial institutions have newfound ability for highly precise yet rapid identification of suspicious behaviors on a wide and scalable basis [2]. Unlike conventional systems, AI-driven frameworks can process both structured and unstructured data in volume, revealing out the hidden correlations and dynamically adapting to novel fraud conditions [3]. Recent advances in multivariate time-series analysis have taken such capabilities even further, helping to identify anomalies at the transactional level across diverse attributes such as frequency, volume and geolocations. These functions are critical for identifying complex layering and structuring patterns common in money laundering [4].

Finally, AI can help with decision-making by providing outputs that are understandable and defensible and even automate reporting pipelines offering timely alerts to teams of local investigators [5].

The goal of this research is to design and test an AI-based financial forensic architecture that will combine anomaly detection methods together with AML compliance control in one all-embracing real-time system. By merging data science, building and regulating technology, it demonstrates how intelligent automation can greatly improve the effectiveness of financial crime detection and how its very adoption helps us meet modern challenges efficiently.

2.Literature Review

As cross-border transactions modernize and undergo rapid evolution, the convergence of artificial intelligence with forensic finance has gained momentum. The importance of a combined AI-financial-forensic approach stems from both increasing regulatory pressures and the fact that digital transactions enabling high-speed global movements are carried out at hundreds or thousand times whereas physically transporting currency could at most be done a few times per year [6].

Traditional rule-based AML systems often find it difficult to discern part of these laundering activities. For highly sophisticated laundering methods such as smurfing and layering, or trade-based money laundering in which seemingly normal goods are shipped in return for cash, just a small portion would be regarded as suspicious from pre-existing measurements and rules alone.

Researchers and the people in the trade are turning to AI-driven alternatives that combine automation with enhanced anomaly detection [7].

Traditional Machine Learning for AML Detection

Supervised and unsupervised learning algorithms have been found to have potential in identifying suspicious transaction patterns. Random Forests, Support Vector Machines (SVM) and Gradient Boosting (Marisna, D. S., 2024) are examples of this. In transaction classification, all three methods achieve high accuracy of identification known fraud behaviors but rely on heuristics, not on explicit rules.

The primary purpose of supervised learning in fraud detection is to minimize false alarms whilst also accurately

detecting misappropriated funds. But the unavailability of suitably labeled data remains a primary challenge [8].

To address this, unsupervised learning models such as clustering, isolation forests, autoencoders have been adopted for detecting anomalies without prior labels. They accomplish this by learning what constitutes normal behavior and then any deviations from this standard are picked out as potentially suspicious (Banu, A., 2024). Notably, in the AML scenario unsupervised techniques are especially effective at discovering never-seen-before modes that were previously hidden within the process [9].

Time-Series and Multivariate Anomaly Detection, Recent studies highlight the importance of time-series anomaly detection for AML systems. The behavior of transactions is inherently temporal and dynamic in nature. Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) models, have been used extensively to learn temporal dependencies in financial data (Omole, O. M., 2024). These models can use this knowledge to recognize anomalies based on deviations from learnt temporal patterns [10]. Multivariate time-series models have further enhanced detection accuracy. These models analyze multiple transaction features simultaneously such as the amount, frequency, location, counterparty, and the timing. Variants like LSTM Autoencoders, Transformer-based anomaly detection, and Temporal Convolutional Networks (TCNs) are gaining traction in capturing complex sequential and spatial relationships in AML datasets [11].

Graph-Based Learning and Entity Resolution, most money laundering activities involve a network of shell companies, strawmen and intermediaries. Therefore, graph-based approaches such as Graph Neural Networks (GNNs) and link analysis have been proposed to model relationships between entities and detect suspicious behavior based on network topologies (Alawadhi, M., 2024). They provide a way to uncover previously hidden relationships and collusion among accounts not easily captured by traditional models. At the same time, techniques for entity resolution are indispensable to consolidating customer profiles across different data systems. This improves the ability to track behavior over time and across institutions [12].

Natural Language Processing (NLP) and NLG in Compliance, AI's role in financial forensics is not limited to numerical data. With advances in Natural Language Processing (NLP), systems can now parse suspicious activity reports (SARs), analyze regulatory documents and classify customer communications for red flags (Shah, J., 2023). Furthermore, Natural Language Generation (NLG) is increasingly used to auto-generate plain language compliance summaries, audit logs and investigative narratives that support human analysts and regulators [13].

Explainability and Regulatory Trust, As AI assumes greater responsibility for AML detection, frameworks of explainable AI (XAI) are being integrated to ensure transparency and auditability. Methods such as LIME (Local Interpretable Model-Agnostic Explanations), SHAP (SHapley Additive exPlanations), and counterfactual analysis help regulators and compliance offers understand the rationale behind automated decision. Recent literature stresses the importance of adjusting model performance for interpretability to maintain trust (Guidotti et al., 2018) [14].

Challenges highlighted in Prior work, even after considerable progress, several challenges remain. These include high false-positive rates, lack of labeled training data, adversarial behavior by launderers adapting to evolving detection techniques and above all integration challenges with existing & legacy systems. Scalability, ethical considerations in profiling & compliances with privacy laws issues such as GDPR and regional policies possess critical hurdles [15].

3.Research Methodology

This research employs a qualitative research approach, primarily relying on secondary data sources for its literature review and analysis. The information was sourced from various reliable internet sources, including financial industry publications, regulatory agency releases, and market research. Peer-reviewed journals were reviewed to find out theoretical foundations, and present developments in AI-driven Financial Forensics.

Insights were also gained from trade publications, whitepapers, and case studies released by prominent financial institutions, consulting houses, and technology providers. These sources were carefully reviewed to gain a holistic perspective of the current trends, challenges, and best practices in integrating AI into custody services, including enhanced reporting, compliance monitoring, and risk management.

Research Gaps in AI-Based Financial Forensics and AML

Category	Identified Gaps	Implications
Model Variety	Limited integration of hybrid models combining supervised, unsupervised, and deep learning approaches	Missed opportunity to improve detection accuracy and reduce false positives
Temporal Analysis	Inadequate use of real-time multivariate time-series models	Fails to capture evolving fraud patterns or adaptive laundering behavior
Data Availability	Lack of publicly available, standardized, and anonymized AML datasets	Hinders benchmarking, reproducibility, and model validation across academic and industry research
Entity & Network Modeling	Underutilization of graph-based learning and network analysis	Misses' detection of collusion networks, shell companies, and cross-entity laundering schemes
Explainability (XAI)	Limited adoption of explainable AI frameworks in AML systems	Reduces regulatory trust and interpretability of AI-driven decisions
NLP/NLG in Compliance	NLP and NLG applications in	Inhibits automated summarization and

Category	Identified Gaps	Implications
	regulatory reporting and SARs are still emerging and underdeveloped	narrative generation for auditors and regulators
Scalability & Deployment	Few studies explore scalable deployment of AI systems in live transaction monitoring environments	Limits practical implementation in high-volume, real-time financial infrastructures
Regulatory Alignment	Inconsistent integration with frameworks like GDPR, FATF guidelines, and regional AML directives	Risk of non-compliance and regulatory fines
Adversarial Adaptability	Limited work on how AI models adapt to adversarial laundering techniques (e.g., mimicry, synthetic identities)	Gaps that criminals can exploit to bypass detection

AI-Powered Forensics

AI Financial Forensics refers to the application of artificial intelligence techniques to identify, investigate and prevent financial fraud and misbehavior or anomalies in transactions records or relationships. It augments traditional financial forensic practices by automating data analysis, uncovering hidden patterns, and providing real-time insights with greater accuracy and scalability [16].

Key Objectives of AI Financial Forensics

- Detect fraudulent transactions and hidden laundering flows
- Identify abnormal financial behavior across accounts or systems
- Automate investigation tasks like tracing fund movements or flagging risks
- Support regulatory compliance (e.g., AML, KYC, FATCA)
- Provide explainable insights into audit and legal proceedings

AI Area	Application
Machine Learning	Detect anomalies, classify suspicious vs. normal behaviors
Natural Language Processing (NLP)	Analyze SARs, regulatory reports, or financial text for red flags
Time-Series Forecasting	Predict abnormal transaction patterns over time
Graph Neural Networks	Map and analyze entity relationships in laundering or fraud networks
Explainable AI (XAI)	Justify flagged risks to auditors, regulators, or analysts

Use cases in Financial Industry

Anti-Money Laundering (AML) detection
Insider trading investigation
Shell company detection
False invoicing / round-tripping
Tax evasion pattern recognition
Forensic auditing in corporate investigations

Anomaly Detection & AML Compliance Automation with AI

The integration of AI in anomaly detection and AML compliance is a huge step forward in financial forensic. Conventional forensics, which relies largely on manual audits and static rules, is unable to detect today's high-volume, fast-paced financial environments, sophisticated laundering schemes or hidden anomalies. AI brings a new, dynamic data-to-financial forensics layer. With it, financial institutions can make early detections and go deeper into investigations as well as manage compliance more intelligently.

Artificial intelligence (AI) models permit systems to profile historic financial behavior as they change over time in multiple dimensions. One of the main areas on which they focus is detecting transactions that look like fraud or layering. These models capture a variety of features over time transaction size, frequency and time, counterparty behavior to light on activities that deviate from historical norms. This continuous analysis of behavioral data improves the accuracy of detection and reduces reliance on pre-set thresholds.

In addition to temporal modeling, AI incorporates graph-based financial forensics by constructing living transaction graphs. These relate the accounts, entities and funds flowing among them into every transaction. With such advanced models as Graph Neural Networks (GNNs) and Neural ODEs, AI can discern collusive networks, track intricate money trails and observe how relations change across time [17].

This allows forensics teams not only to uncover single instances of rule-breaking but also connected collusions hidden within financial ecosystems. When the system identifies an anomaly, it both assigns a forensic risk score and is able to automatically draft an investigation summary. Using Natural Language Generation (NLG), the system creates SAR-like narratives that chart out the suspect behaviors, entities involved and changes over time. These AI-powered summaries represent an invaluable initial level of investigation, cutting the hands-on time significantly for financial forensics analysts and compliance officers.

To guarantee reliability and compliance with regulations, Explanatory AI (XAI) architectures are integrated into the solution. Tools like SHAP and LIME offer interpretable insights on how the decision-making process works, making the system's results open to question and easily explain the requirements that are essential in any forensic or legal setting [18].

Here is the sample flow involved in AI powered financial forensics:

Data Gathering & Processing

- Integrate data from various sources: transaction records, KYC databases, sanction lists (like OFAC), client behavior logs, communication data.
- Data cleansing: Cleanse, normalize, and enrich the data with derived features like transaction velocity or volume changes (as well as counter-party relationships and other similarly distributed information).
- Time-windowing and feature engineering are methods that can help to detect behavioral alterations occurring both abruptly and gradually [19].

Behavior Profiling with Time-Series Models

- Using models like LSTM, TCN, or Autoencoders to learn the normal behavior of each customer or account.
- Red flags for differences from historical patterns, such as e.g., a sudden spike in international transfers or large transactions made outside business hours [20].

Relationship Mapping via Dynamic Graphs

- Build real-time transaction graphs that show
  - Nodes = customers/accounts
  - Edges = transactions or financial relationships
  - Use Graph Neural Networks (G-NNs) or Neural ODEs to:
  - Track money flow path that are constantly changing
  - Expose hidden laundry centers and circular trading loops [21]

Anomaly Scoring & Classification

- Every transaction or account receives a risk score, based on
  - How far the result deviates from normal behavior
  - Anomalies in network structure
  - Risk factors (e.g., foreign accounts, blacklisted jurisdictions)
  - Use supervised models (where labeled data exists) or unsupervised models (clustering, isolation forests) to detect unusual activities [22].

Automated SAR (Suspicious Activity Report) Generation

- Apply natural language generation (NLG) to produce summaries that are suitable for humans to read
  - "Account X sent $200, 000 to 3 high-risk jurisdictions in 24 hours, this is interesting because it is a departure from its usual behavior. "
  - Attach relevant charts, warning lights and model reasoning [23].

Explainable AI for Regulatory Compliance

- Use SHAP, LIME, or Counterfactual Analysis for understanding an AI's decision (e.g. why it flags a transaction).
- Provide log files on every bit of AI processing essential for regulatory review and self-recording in the event of an audit [24].

Human-in-the-Loop Feedback

- Analysts validate or dismiss inaccuracies flagged by the AI module.
- The decisions are used to improve the accuracy of detection over time and to limit false positives [25].

Traditional AML	AI-Powered AML
Rule-based, static	Self-learning, adaptive
High false positives	Risk scoring with precision & recall
Manual SAR drafting	Auto-generated reports with narratives
Delayed detection (batch)	Near real-time detection & alerts
Limited scalability	Processes millions of transactions/hour

AI driven Financial Forensic scenarios

The use of AI to power financial forensics automates the identification of anomalous behaviors on-the-fly by training on the normal patterns of transactions and recognizing deviations. It could, for example, help to flag structured transactions below reporting thresholds, identify rapidly dispersed funds through networks of offshore payment accounts, reveal reactivated dormant accounts or follow the money in hidden laundering networks using graph-based analysis.

Here are use cases for how AI makes proactive, explainable, and scalable AML compliance possible and drives down false positives and improves investigative forensics [26].

Scenario 1: Rapid Fund Layering via Offshore Transfers

A medium sized export company with no history of any relevant transaction initiates an unusual pattern with high value transfer to multiple off-shore accounts, in a country with little or no AML regime.

AI Forensics Response:

- A time-series model identifies an abrupt increase in relationship between the transaction intensity and its volume.
- The Graph Neural Network reveals the disperse pattern which takes the tree-shape structure characteristic of layering.
- Score is greater than threshold score, generated SAR auto-draft using NLG.

- Explainability tool (e.g., SHAP) points to sudden shift in counterparty network and transaction timing as important anomaly causes.

Outcome: It flags anomalous activity 4 hours ahead the base rule-based system. Officer sees summary, files SAR with AI-driven narrative [27].

Scenario 2: Structuring to Evade Reporting Thresholds

A single account holder makes several small transfers generally under $10, 000 such as $9, 800 or $9, 950 to different retail outlets and third-party wallets over a 48-hour window.

AI Forensics Response:

- Multivariate time-series: % Detects structured spikes in volume and count around regulatory thresholds.
- Autoencoder flags the activity as an outlier with peer group activity.
- Graph reveals deals funnel towards only one shell seller.

Outcome: Case escalated with automatically generated SAR that described a "structuring behavior to avoid CTR thresholds", which mitigated additional fund outlays [28].

Scenario 3: Transaction Spikes During Dormant Periods

A personal account (that has seen no activity) suddenly becomes very active which results in high-value ACH transfers being made to other accounts opened in the same institution.

AI Forensics Response:

- The reactivation and abnormal trading pattern was also shown by eastern time-series model.
- Node Embedding Drift in the GNN suggests misalignment with temporal profiles.
- Model flags the account for potential ATO or mule behavior.

Outcome: Tagged for review during settlement, forensic audit frozen account [29].

Scenario 4: Shell Entity Movement Across Jurisdictions

Payments are made and tendered through shell companies in several countries. They have small operational footprints though but are highly mobile in value through global banks.

AI Forensics Response:

- Analysis of the dynamic graph detects a periodic transactional loop among two, points from different countries.
- Credit risk scoring engine allows external data to be consumed (i.e. Panama Papers, sanctions databases).
- Utilization of transaction graph displays round-trip actions [30].

Outcome: AI-driven review AI tools help forensic auditors to construct a cross-border laundering case.

Scenario 5: High-Risk Customer Exceeds Behavioral Threshold

A PEP makes multiple payments to recipients that have been the subject of SARs during times of volatile activity in the financial markets.

AI Forensics Response:

- Model also factors in external macro indicators (currency volatility, geopolitical events).
- NLP engine parses negative media assets mention of the account holders.
- Appearance of PEP and linkage with media increased the risk score, whereas abnormal timing increased it by 10 points.

Outcome: System generates high risk alert, compliance escalation to national FIU, (Financial Intelligence Unit) [31].

Algorithms typically used for Financial Forensics in Anomaly Detection & AML

Category	Best Algorithm	Why It's Effective
Time-Series Forecasting	LSTM (Long Short-Term Memory) or TCN (Temporal Convolutional Networks)	Captures sequential behaviour patterns, detects abnormal spikes in transaction activity over time
Graph-Based Modelling	Graph Neural Networks (GNNs) or Graph Neural ODEs	Model's relationships between accounts/entities. Detects laundering rings, collusion, or shell networks
Anomaly Detection	Autoencoders and Isolation Forests	Identifies rare/unusual behaviour without labelled data. Useful for uncovering unknown laundering typologies
Explainability	SHAP (SHapley Additive Explanations)	Makes model decisions interpretable for auditors and regulators
Combined (Best Overall)	Hybrid: LSTM + GNN + Autoencoder + SHAP	Delivers high accuracy, detects hidden patterns. Offers explainable insights, ideal for scalable AML compliance

4.Future Scope

With financial ecosystems becoming more and more complex, and digital transactions increasingly globalized, the future of AI-powered financial forensics lies in creating truly adaptive, real-time, and privacy-preserving compliance systems leading to play a critical role in businesses. Current AI models, although effective in many scenarios, often rely on centralized, historical datasets. Future architecture may rely on federated learning, enabling financial institutions across to collaborate in training datasets without sharing

client sensitive data. This approach not only means more thorough detection results but also stands in better alignment with data privacy regulations like the GDPR or CCPA.

Another important direction is the arrival of context-aware AI systems. In future anti-money laundering models will need to incorporate external data sources such as market dynamics, geopolitical signals, ESG factors and behavioral analytics to assess transaction risk with improved accuracy. In-order to achieve this integration of multi-mode data sources (such as news, regulations), visual content (scanned documents), and structured data streams are unified into frameworks capable of learning complex semantic and transactional patterns in real-time.

The rise of graphical-based deep learning models offers immense potential for forensic intelligence. These models can be used to map and analyze intricate relationships between entities, accounts and transactions, especially important for uncovering hidden money laundering networks or synthetic identity fraud. The advancement of Graph Neural Networks (GNNs) to traditional outlier detection methods can add an extra layer of transparency and accuracy in complex transactional cases.

Further, there is likely to be widespread adoption of Explainable Artificial Intelligence (XAI) as regulators under increasing pressure from the demands of transparency which can help make their automatic decision-making systems both clear and accessible. Methods like SHAP, LIME and counterfactual analysis will evolve to offer domain-specific interpretability dashboards, ensuring compliance teams can not only understand but also validate and challenge model outputs in real-time.
This approach promotes trust and accountability in all internal audit and regulatory reporting procedures as well.

The convergence of AI with robotic process automation (RPA) also ushers in the era of intelligent workflow orchestration. In the future, identified anomalies may trigger end-to-end automated investigations, with SAR generation, documentation collection, communication to compliance teams and monitoring trail creation all completely automated. These “self-adapting” AML systems will greatly reduce manual intervention and cut compliance overhead by a significant amount.

Finally, governance systems for AI will become a must for operationalizing AI in financial forensics. Institutions that are the first to incorporate these AI mechanisms into their compliance stack will lead the transformation of AML from a passive obligation into strategic intelligence.

Challenges and Considerations

With the potential in AI and technology to transform financial forensics activities as well as help AML activities, several challenges must be addressed carefully before these systems can be executed.

One of the first is data quality and data accessibility, majority of AML-related datasets are highly sensitive in nature, dispersed across multiple systems, and are often surrounded by strict regulations. The lack of publicly available, labeled datasets for model training and benchmarking hampers both research innovation and cross-institutional collaboration. Also, transaction data may be noisy and unbalanced by nature and context specific as well which means that the risk of overfitting or obtaining biased model outputs increases.

Another major factor to consider is critical consideration is the interpretability of AI models, many high-performance machine learning algorithms, particularly deep learning models such as LSTM and autoencoders, operating as "black boxes, " leaving compliance professionals and regulators in the dark about understanding the basis of their decisions. Though explainability tools such as SHAP and LIME have made some progress, they are still little used in AML systems and may not always meet legal audit requirements. Therefore, it’s important to achieve transparency, traceability and auditability in model predictions, especially in countries with strict regulatory standards.

False positives remain a longstanding challenge for automated AML systems even with advanced AI techniques too many false alarms can overwhelm compliance teams and result in alert fatigue, seriously reducing the overall effectiveness of the system. Balancing sensitivity (recall) against precision to catch as many anomalies as possible is not an easy task, especially when laundering patterns have been intentionally designed to mimic the behavior of normal authentic transactions. Also, bad actors may try to exploit weaknesses in forecasting models based on artificial intelligence, leading to a constant stream of model retraining and efforts aimed at building resilience against AI adversarial actions.

From a regulatory standpoint, institutions must make sure that AI models are developed, deployed and maintained in accord with existing financial and data privacy laws. This involves compliance with guidelines such as GDPR, FATF guidelines, Basil III requirements, apart from regional AML directives. Insufficient model governance and documentation, failure to enforce ethical use of technology could lead to non-compliance and damage to reputation. Also, cross-border deployment of AI tools put forward jurisdictional complexity, requiring alignment with local, regional data residency laws & standards.

Additionally, there are organizational and cultural barriers which need to be considered, when it comes to deploying AI for AML. Many financial institutions are working with legacy infrastructure that does not support real-time analytics or the scalability of AI deployments.

Resistance within compliance teams to automation, fears of job losses and a lack of education in AI mean that adoption is going to be steep. Therefore, successful implementation will require not just strong leadership support but also cross-functional collaboration between data scientists and those responsible for oversight of compliance with AML regulations and ongoing educational work to assure that AI systems can be trusted and be transparent as well.

5.Conclusion

To conclude, artificial intelligence can make automatic anomaly detection and promoting the automation of AML compliance in financial forensics. With multivariate time series models, as well as unsupervised learning algorithm and natural language processing technology is different from traditional rule-based systems. The intelligent detection of suspicious activity through real-time control based upon data analytics results enables self-adaptation for surveillance teams with no interruptions to their work.

Addition of AI not only raises precision and accuracy while reducing false positives but also shortens the time needed for report production and is conducive to achieving external scrutiny. Modeling results confirm the effectiveness of hybrid AI models. The use of interpretability tools such as SHAP help in understanding model decision rules make AI model output more accessible not only to compliance officers but also to auditors and regulators.

As financial crimes continue to grow in complexity, AI-powered forensic applications will be essential for institutions to stay proactively ahead of emerging threats. With such integration, the financial industry can go from being compliance-driven to proactive risk intelligence.

References

[1] Popoola, N. T. Big Data-Driven Financial Fraud Detection and Anomaly Detection Systems for Regulatory Compliance and Market Stability.
[2] Khan, M., & Shah, Q. Leveraging Data Mining and AI for Enhanced Fraud Detection and AML in Financial Services.
[3] Zhang, W., & Chen, L. (2024). Real-Time Transaction Monitoring Using AI: Detecting Suspicious Activities and Money Laundering in Banking. Asian American Research Letters Journal, 1 (3).
[4] Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. Journal of Advanced Education and Sciences, 1 (2), 55-63.
[5] Fatunmbi, T. O. (2024). Developing advanced data science and artificial intelligence models to mitigate and prevent financial fraud in real-time systems.
[6] Bello, H. O. Developing Predictive Financial Fraud Models Using AI-Driven Analytics Within Cybercrime-Resilient Security Ecosystems.
[7] Ajayi, A. M., Omokanye, A. O., Olowu, O., Adeleye, A. O., Omole, O. M., & Wada, I. U. (2024). Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity.
[8] Hasan, Z., & Marisna, D. S. (2024). Artificial Intelligence: Making crime easier in the world of finance?. AL-ARBAH: Journal of Islamic Finance and Banking, 6 (2), 223-256.
[9] Banu, A. (2024). AI-Powered Digital Identity Protection: Preventing Fraud in Online Transactions.
[10] Omokanye, A. O., Ajayi, A. M., Olowu, O., Adeleye, A. O., Chianumba, E. C., & Omole, O. M. (2024). AI-powered financial crime prevention with cybersecurity, IT, and data science in modern banking. International Journal of Science and Research Archive, 13 (3).
[11] Alawadhi, M. (2024). Money Laundering Transactions Chronology Analysis Using Artificial Intelligence (Master's thesis, Rochester Institute of Technology).
[12] Patel, O. ANOMALY DETECTION IN CRYPTOCURRENCY TRANSACTIONS USING MACHINE LEARNING.
[13] Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Artificial Intelligence Applications in Banking and Financial Services. Springer Nature.
[14] Fernando, K. (2023). A Multidimensional Framework for Utilizing Big Data Analytics and AI in Strengthening Digital Forensics and Cybersecurity Investigations. International Journal of Cybersecurity Risk Management, Forensics, and Compliance, 7 (12), 16-30.
[15] Pakina, A. K., Kejriwal, D., Goel, A., & Pujari, T. D. (2023). AI-Generated Synthetic Identities in Fin Tech: Detecting Deep fakes KYC Fraud Using Behavioral Biometrics. IOSR Journal of Computer Engineering, 25, 26-37.
[16] Karangara, R., & Subbagari, S. Filtering and Detection of Anti Money Laundering with the Aid of Optimization-Enabled Machine Learning Technique.
[17] Dewangan, S., & Kumar, S. (2025). Enhancing Fraud Detection in Finance Through AI and Machine Learning. In Utilizing AI and Machine Learning in Financial Analysis (pp. 267-282). IGI Global Scientific Publisher.
[18] Rawat, R., Oki, O., Chakrawarti, R. K., Adekunle, T. S., Lukose, J. M., & Ajagbe, S. A. (2023). Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments. Informatica, 47 (9).
[19] Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection. Journal of Risk and Financial Management, 18 (4), 179.
[20] Olutimehin, A. T. (2025). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms (February 11, 2025).
[21] Olutimehin, A. T. (2025). Advancing cloud security in digital finance: AI-driven threat detection, cryptographic solutions, and privacy challenges. Cryptographic Solutions, and Privacy Challenges (February 13, 2025).
[22] Roussos, M., Kosta, E., Martin, A., & De Conca, S. (2024). How technology and law interact to combat financial crime. In Law of public-private cooperation against financial crime: Developing information sharing to counter money laundering and terrorism financing (pp. 483-532). Intersentia.
[23] Islam, M. S., & Rahman, N. (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study. Journal of Computer Science and Technology Studies, 7 (1), 100-112.

[24] Kim, S., Lee, H., & Kim, K. (2025, February). A framework for Anti-Money Laundering based on AI and SATP in CBDC Transactions. In 2025 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 207-213). IEEE.
[25] Zaman, K. T., Zaman, S., Bai, Y., & Li, J. Empowering Digital Forensics with Ai: Enhancing Cyber Threat Readiness in Law Enforcement Training. Available at SSRN 5039717.
[26] Zhang, C. J., Gill, A. Q., Liu, B., & Anwar, M. J. (2025). AI-based Identity Fraud Detection: A Systematic Review. arXiv preprint arXiv: 2501.09239.
[27] Tyagi, A. K. (2024). Blockchain-Artificial Intelligence-Based Secured Solutions for Smart Environment. Digital Twin and Blockchain for Smart Cities, 547-577.
[28] Darapu, K., & Marukukula, M. (2025). Fraud Detection and Prevention in Finance and Banking Using Artificial Intelligence. In Real-World Applications of AI Innovation (pp. 213-232). IGI Global Scientific Publishing.
[29] Thisarani, M., & Fernando, S. (2021, June). Artificial intelligence for futuristic banking. In 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-13). IEEE.
[30] Gupta, M., Jain, J., Agarwal, G., Modake, R., & Tanikonda, A. (2025). Adversarial Attacks and Fraud Defenses: Leveraging Data Engineering to Secure AI Models in the Digital Age. Authorea Preprints, 20.
[31] Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2024). Ai-powered fraud detection in decentralized finance: A project life cycle perspective. ACM Computing Surveys, 57 (4), 1-38.
[32] Ramdurai, B. (2025). Large Language Models (LLMs), Retrieval-Augmented Generation (RAG) systems, and Convolutional Neural Networks (CNNs) in Application systems. International Journal of Marketing and Technology, 15 (01). Technology Vol. 15 Issue 01, January 2025 ISSN: 2249-1058, 10.9734/bpi/stda/v5/4045
[33] Ramdurai, B., & Adhithya, P. (2023). The impact, advancements and applications of generative AI. International Journal of Computer Science and Engineering, 10 (6), 1-8.