Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

AI-Driven KYC & AML Automation: A New Frontier for Regulatory Compliance

Ravindra Reddy Madireddy

Independent Researcher, USA

ARTICLE INFO

Received: 03 Nov 2025

Revised: 04 Dec 2025

Accepted: 14 Dec 2025

ABSTRACT

Financial institutions are under increasing pressure to manage KYC and AML compliance requirements effectively. Rule-based systems operating under traditional setups cause too many false alarms and have difficulty identifying complex money laundering operations. Besides, the manual verification processes eat up a lot of resources and make the onboarding of new customers take longer. Because compliance is so resource-intensive in the traditional way, there is room for AI to take over. Machine learning techniques interrelate transaction patterns on so many levels at the same time.NLP engines take the load off by extracting information from different document types in a more straightforward way. Computer vision systems can handle identity document verification irrespective of any variations specific to a certain jurisdiction. Graph neural networks unearth the links between nodes that show networked illicit activities. Deep learning structures respond to the changes in money laundering methods without the need for human rule updates. Explainable AI tools give insight into the automated decision-making processes.SHAP values and LIME methods break down predictions into easily understandable feature contributions. A human-in-the-loop system gathers expert opinion for continual model improvement. Governance structures are there to ensure the responsible implementation on strategic, tactical, operational, technical, and ethical levels.

Keywords: Anti-Money Laundering, Know Your Customer, Machine Learning, Graph Neural Networks, Explainable Artificial Intelligence, Regulatory Compliance

I. Introduction

The move from a compliance approach, which is mostly reactive, to one based on intelligence-led capabilities that are proactive is a tectonic shift in the fight against financial crime. AI-powered automation is the way that allows institutions to respond to a growing list of regulatory demands while also enabling them to lower their operational costs and improve their detection efforts in different risk scenarios. Financial institutions carry out countless compliance checks every year. KYC and AML represent a heavy burden in terms of the human and computational resources needed for customer onboarding, monitoring, and investigations. The trend is that compliance costs are going up as the regulatory frameworks become more complex and enforcement actions more vigorous. The costs associated with regulations extend beyond the direct operational expenses to technology investments and staff training programs that follow regulatory examination activities. Traditional verification methods create significant delays in customer acquisition processes. Manual review

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

procedures demand extensive oversight by compliance personnel across multiple verification stages [1].

Conventional methods depend on rule-based engines that match predefined patterns with customer data and transaction histories. These types of systems take into account structured data fields, for instance, names, addresses, dates of birth, and ID numbers by means of deterministic logical pathways. Document verification problems hamper the increase in operational inefficiencies. Institutions must process identity documents from numerous jurisdictions. Each jurisdiction presents unique formats, security features, and data field arrangements. Standardized automated extraction remains difficult to achieve across this document's diversity. Rule-based systems handle structured inputs adequately but demonstrate significant limitations. Processing diverse document formats requires extensive programming adjustments. Interpreting contextual risk factors demands human judgment that automated rules cannot replicate. Adapting to emerging typologies necessitates constant system updates and maintenance [1].

Machine learning applications in watch-list filtering demonstrate potential for improving compliance accuracy. Traditional name-matching algorithms produce excessive false alerts during sanctions screening processes. These false positives burden compliance teams with unnecessary investigation workload. Research into supervised learning techniques shows promise for reducing alert volumes while maintaining detection effectiveness. Classification models trained on historical screening decisions learn patterns distinguishing genuine matches from spurious alerts. Feature engineering approaches consider phonetic similarities, cultural naming conventions, and address formatting variations across different regions [2].

Regulatory expectations expand beyond simple transaction monitoring frameworks. Modern compliance requirements mandate comprehensive risk assessment methodologies. Beneficial ownership structures extending through multiple corporate layers require detailed analysis. Politically exposed person affiliations across immediate family members and close associates demand a thorough investigation. Complex cross-border relationships involving correspondent banking networks present additional screening challenges. Adverse media screening across multiple languages and jurisdictions requires sophisticated natural language processing capabilities. Sanctions screening involves real-time comparison against extensive lists of designated entities and individuals. Geopolitical situations evolve continuously, requiring frequent updates to screening databases [2].

The complexity inherent in modern compliance operations creates opportunities for AI-driven automation. Machine learning systems can learn from historical patterns embedded in past investigations and determinations. Natural language processing techniques interpret unstructured information across document types and languages. Contextual decision-making incorporating multiple risk dimensions becomes feasible through advanced analytics. Tasks previously requiring human expertise and institutional knowledge accumulated over years of compliance experience become candidates for intelligent automation. The transition from rule-based processing to adaptive learning systems represents a fundamental shift in compliance technology architecture.

II. Related Work

Prior literature on AML compliance automation focused predominantly on isolated machine learning applications addressing specific detection challenges. Early implementations applied supervised classification algorithms to transaction monitoring tasks with limited consideration for explainability requirements. Graph-based detection methods emerged separately from behavioral analytics

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

frameworks without integrated architectural designs. Document verification systems were developed independently from risk assessment engines, creating operational silos.

Recent advances demonstrate increased interest in end-to-end compliance automation. Blockchain transaction analysis employs graph neural networks, revealing complex fund flow patterns. Time-frequency analysis techniques identify structuring behaviors through wavelet transformations. Watch-list filtering applies natural language processing, reducing false match rates during sanctions screening. Face verification leverages deep learning for identity document validation across diverse jurisdictions.

The article synthesizes disparate technical developments into a comprehensive AI-driven compliance architecture. Key contributions include integration of document intelligence, behavioral analytics, and autonomous decision agents within unified operational frameworks. The proposed architecture combines computer vision for identity verification, graph neural networks for relationship analysis, and reinforcement learning for adaptive risk classification. Human-in-the-loop mechanisms balance automation efficiency with expert oversight requirements.

Explainability frameworks addressing regulatory transparency receive particular emphasis. SHAP values, LIME techniques, and attention mechanisms provide interpretable outputs satisfying audit requirements. Five-layer governance systems delineate the oversight features throughout strategic, tactical, operational, technical, and moral dimensions. Additionally, they have continuous monitoring mechanisms to spot version degradation and ensure performance stability towards the ever-changing threat panorama.

III. Limitations of Conventional Compliance Systems

Rule-Based Processing Constraints

Traditional KYC and AML platforms operate on deterministic logic. Compliance officers define specific conditions that trigger alerts or escalations. These systems excel at identifying exact matches in sanctions lists. Transaction monitoring flags activities exceeding predefined thresholds with consistent accuracy. However, the reliance on static rules creates significant operational challenges. Document variability across jurisdictions presents fundamental processing obstacles. Passports from different countries present information in varying formats and layouts. Utility bills lack international standardization across service providers. Corporate documents differ significantly across legal systems and registration frameworks.

Each format variation requires additional rule creation within the compliance infrastructure. Systems accumulate thousands of interconnected conditions over time. Rule maintenance becomes increasingly complex as regulatory requirements expand. Optimization efforts face diminishing returns as rule sets grow larger. The interdependencies between rules create unintended consequences when modifications occur. Testing new rules against existing logic demands extensive validation cycles. Legacy rules remain embedded in production systems long after their original purpose becomes obsolete. Documentation of rule rationale deteriorates as compliance teams experience personnel turnover.

Time-frequency analysis approaches reveal limitations in traditional transaction monitoring methods. Conventional systems examine individual transactions in isolation without considering temporal patterns. Suspicious behavior often manifests through frequency changes in transaction activity over specific time periods. Structuring activities involves breaking large amounts into smaller transactions spread across multiple days or weeks. Traditional threshold-based rules fail to detect these distributed

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

patterns effectively. Wavelet transformation techniques enable simultaneous analysis of transaction amounts and timing characteristics. Short-time Fourier transforms capture periodic patterns that indicate coordinated activity across multiple accounts [3].

Static Risk Assessment Frameworks

Conventional systems apply risk ratings through static matrices. Predetermined attributes drive score assignments across customer populations. Geographic location contributes fixed values regardless of individual circumstances. Industry sector classifications carry standardized risk weightings across all business types. Transaction volume ranges trigger mechanical score increases without contextual analysis. This approach fails to capture behavioral dynamics emerging over time. Temporal patterns revealing gradual changes in customer activity remain invisible to static scoring methodologies. Relationship networks connecting multiple entities escape detection when risk assessment focuses solely on individual account attributes.

Money laundering schemes continuously evolve in response to detection capabilities. Blockchain-based cryptocurrencies introduce additional complexity to traditional AML frameworks. Digital asset transactions occur outside conventional banking infrastructure. Pseudonymous addresses obscure true beneficial ownership and transaction purposes. The immutability of blockchain records provides permanent audit trails but requires specialized analytical techniques. Traditional rule-based systems cannot effectively process blockchain transaction graphs or identify mixing services designed to obscure fund origins [4].

Machine learning applications in cryptocurrency monitoring face unique challenges. Supervised learning models require labeled training data indicating confirmed money laundering cases. Such labeled datasets remain scarce due to investigation complexity and confidentiality requirements. Semi-supervised learning techniques attempt to leverage small amounts of labeled data alongside larger unlabeled transaction sets. Graph neural networks analyze blockchain transaction flows across multiple addresses and wallets. Feature engineering extracts relevant patterns from transaction metadata, including timing, amounts, and address clustering behaviors. The label scarcity problem limits model accuracy and requires innovative approaches combining multiple detection methodologies [4].

Challenge Category	Limitation Description	Impact on Operations
Document Processing	Format variations across jurisdictions	Requires extensive rule creation for each document type
Risk Assessment	Static scoring matrices	Cannot capture behavioral dynamics or temporal patterns
Alert Generation	Threshold-based triggers	Produces excessive false positives requiring manual review
Pattern Detection	Individual transaction analysis	Fails to identify distributed structuring activities
System Maintenance	Rule interdependencies	Creates optimization difficulties as conditions accumulate
Adaptation Speed	Manual updates required	Detection gaps persist until new typologies are programmed

Table 1. Limitations of Rule-Based Compliance Systems [3, 4].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

IV. AI-Enabled Compliance Architecture

Document Intelligence and Identity Verification

Computer vision models trained on diverse identity documents extract relevant fields regardless of format variations. Modern deep learning architectures process multiple languages simultaneously within unified processing pipelines. Security features embedded in official documents require sophisticated detection mechanisms. Face verification represents a critical component of identity document validation. Deep learning approaches to face recognition have evolved significantly through joint learning objectives that combine identification and verification tasks simultaneously [5].

Face identification involves recognizing specific individuals from large candidate sets. Face verification is the process by which it is established whether two face images are of the same person. Conventional methods considered these tasks as different ones and hence used different model architectures. Joint learning frameworks leverage complementary information from both objectives during training. The identification supervision signal provides rich discriminative information across numerous identity classes. Verification supervision encourages learned representations to capture subtle differences distinguishing similar faces. Combining these learning signals produces more robust feature representations than either task alone [5].

Convolutional neural network architectures extract hierarchical visual features from face images. Early layers capture low-level patterns, including edges and textures. Middle layers detect facial components such as eyes, noses, and mouths. Deeper layers encode holistic facial structure and identity-specific characteristics. The learned representations map face images into compact embedding spaces where distances reflect identity similarity. Faces belonging to the same individual cluster closely together. Faces from different individuals occupy distant regions within the embedding space [5].

Natural language processing engines parse unstructured proof-of-address documents. Utility bills present diverse layouts across service providers and geographic regions. Named entity recognition identifies relevant verification elements, including addresses, dates, and account holder names. Consistency validation compares extracted information against customer-provided declarations. While automated self-belief ratings do not meet recognition thresholds, reviewers review discrepancies in addition.

Behavioral Analytics and Anomaly Detection

Unsupervised learning algorithms establish baseline behavioral profiles for customer segments. Graph neural networks analyze relationship networks across cryptocurrency transaction flows. Blockchain technology creates permanent records of all transactions between digital wallet addresses. These transaction networks form complex graph structures requiring specialized analytical techniques. Traditional machine learning approaches struggle with graph-structured data containing relational dependencies. Graph neural networks operate directly on network topologies to extract meaningful patterns [6].

Message passing architectures aggregate information from neighboring nodes in transaction graphs. Each node represents a cryptocurrency address or wallet. Edges capture fund transfers between addresses with associated metadata. Node features encode transaction amounts, timing patterns, and historical activity summaries. Graph convolutional layers propagate information across network connections iteratively. Multiple propagation rounds enable the detection of patterns spanning several transaction hops. The learned node representations incorporate both local transaction behavior and broader network context [6].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Cryptocurrency mixing services deliberately obscure transaction origins through complex forwarding chains. Funds are split across multiple intermediate addresses before reaching final destinations. Graph neural networks identify suspicious structural patterns characteristic of mixing operations. Temporal analysis captures timing coordination across related transactions. Address clustering techniques group wallets controlled by single entities, despite appearing as separate accounts. The combination of graph topology and temporal features improves detection accuracy beyond methods considering either dimension independently [6].

Supervised learning requires labeled examples distinguishing legitimate transactions from money laundering activities. Ground truth labels remain scarce due to investigation complexity and confidentiality constraints. Semi-supervised approaches leverage unlabeled transaction data alongside limited confirmed cases. Graph-based propagation spreads label information through network connections based on structural similarity. Nodes connected to known illicit addresses receive higher suspicion scores through iterative refinement processes [6].

Technology Component	Primary Function	Application Domain
Computer Vision	Document field extraction	Identity verification across multiple formats
Face Recognition	Biometric matching	Photograph validation against submitted images
Natural Language Processing	Unstructured text parsing	Proof-of-address document analysis
Graph Neural Networks	Network analysis	Cryptocurrency transaction flow mapping
Unsupervised Learning	Baseline profiling	Customer behavioral pattern establishment
Recurrent Neural Networks	Time series processing	Temporal transaction pattern detection

Table 2. AI Technologies for Compliance Automation [5, 6].

V. Autonomous Decision Agents for Risk Classification

AI agents equipped with machine learning capabilities navigate complex decision trees considering multiple risk factors simultaneously. Transaction monitoring systems traditionally relied on rule-based threshold mechanisms, generating excessive false positives. Machine learning applications in AML transaction monitoring address limitations inherent in conventional rule-based approaches. Supervised learning algorithms, including random forests, support vector machines, and gradient boosting methods, classify transactions based on historical patterns. These algorithms learn decision boundaries from labeled training data containing confirmed suspicious and legitimate transaction examples [7].

Deep learning architectures process high-dimensional transaction features through multiple hidden layers. Artificial neural networks capture nonlinear relationships between transaction attributes and money laundering risk. Feature engineering remains critical for model performance. Transaction amount patterns, counterparty relationships, geographic information, and temporal characteristics contribute to predictive accuracy. Natural language processing techniques analyze unstructured text data from transaction descriptions and customer communications. Sentiment analysis identifies unusual language patterns potentially indicating fraudulent intent [7].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Ensemble strategies combine multiple base classifiers to improve the usual prediction reliability. Different algorithms exhibit varying strengths across transaction types and risk scenarios. Bagging approaches train multiple models on bootstrapped data samples. Boosting methods sequentially focus on misclassified examples from previous iterations. Model aggregation through voting or weighted averaging produces more robust predictions than individual classifiers. Cross-validation techniques assess generalization performance, preventing overfitting to training data peculiarities [7].

Human-in-the-loop architectures contain expert comments in automated anomaly detection workflows. Anomaly detection structures flag unusual patterns deviating from installed behavioral norms. But, now, not all anomalies constitute authentic threats requiring research. Domain experts possess contextual knowledge enabling accurate interpretation of flagged cases. Interactive toolkits facilitate collaboration between automated systems and human analysts during anomaly investigation processes. Visual analytics interfaces present detected anomalies alongside relevant contextual information supporting analyst decision-making [8].

Explanation mechanisms provide transparency into automated anomaly detection reasoning. Analysts require an understanding of why specific transactions triggered alerts. Feature importance visualizations highlight which transaction attributes contributed most significantly to anomaly scores. Counterfactual explanations demonstrate how transaction characteristics would need to change for reclassification as normal activity. These explanations build trust in automated systems while enabling analysts to identify systematic errors requiring model refinement [8].

Action recommendation systems suggest appropriate responses to detected anomalies. Different anomaly types require different remediation strategies. Some anomalies warrant immediate transaction blocking while others necessitate enhanced monitoring or customer outreach. The system learns optimal action policies through feedback regarding intervention outcomes. Analysts provide structured feedback confirming or correcting recommended actions. This feedback refines action selection policies over time, improving alignment with organizational risk management objectives [8].

Workflow integration embeds anomaly management capabilities within existing operational processes. Analysts access anomaly investigation tools through unified interfaces, minimizing context switching. Case management systems track investigation progress and resolution status. Collaboration features enable knowledge sharing across analyst teams. Historical case repositories preserve institutional knowledge regarding anomaly interpretation and response strategies. Continuous learning mechanisms incorporate analyst feedback, updating detection models and action recommendation policies based on accumulated operational experience [8].

Method Category	Technique	Operational Benefit
Supervised Learning	Random forests, gradient boosting	Classification based on historical patterns
Deep Learning	Artificial neural networks	Nonlinear relationship capture
Ensemble Methods	Model aggregation through voting	Improved prediction reliability
Anomaly Detection	Statistical outlier identification	Unusual pattern flagging
Active Learning	Uncertainty sampling	Strategic case selection for expert review
Interactive Learning	Online parameter updates	Continuous refinement from analyst feedback

Table 3. Machine Learning Approaches for Risk Classification [7, 8]

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

VI. Governance, Explainability, and Regulatory Considerations

Model Transparency Requirements

Regulatory frameworks increasingly require financial institutions to explain compliance decisions. Customer relationship declinations demand clear justification. Suspicious activity reports filed with regulatory authorities must demonstrate sound reasoning. AI systems must provide interpretable outputs that compliance officers and regulators can understand and validate. Deep learning models achieve high accuracy but operate as black boxes, obscuring decision logic. Explainable artificial intelligence techniques address this transparency challenge by revealing how models arrive at specific predictions [9].

Attention mechanisms in neural networks highlight which features most influenced particular decisions. Document analysis models assign importance weights to different text segments or image regions. Transaction monitoring systems identify which behavioral patterns triggered anomaly alerts. These attention maps provide visual explanations showing compliance officers exactly where models detected suspicious indicators. Layer-wise relevance propagation traces prediction contributions backward through network layers. Each intermediate representation receives relevance scores indicating its contribution to final outputs [9].

SHAP values decompose model predictions into characteristic contributions. Each transaction attribute receives a score indicating its positive or negative influence on money laundering probability estimates. Features pushing predictions toward suspicious classifications receive positive SHAP values. Features suggesting legitimate activity receive negative scores. The sum of all feature contributions equals the difference between the model prediction and the average baseline prediction. This additive property enables intuitive interpretation of how different factors combine to produce overall risk assessments [9].

LIME techniques generate local approximations of complex model behavior. The method creates interpretable linear models explaining predictions for specific instances. Perturbed versions of original inputs test model sensitivity to feature variations. Linear regression fits approximate decision boundaries in the local neighborhood surrounding instances of interest. This locally faithful approximation reveals which features dominate decisions for particular cases even when global model behavior remains highly nonlinear [9].

Validation and Continuous Monitoring

AI compliance systems require rigorous validation frameworks assessing model performance across demographic segments. Fairness concerns call for the same treatment regardless of the included attributes. Discriminatory outcomes create legal responsibility and reputational damage. Performance monitoring tracks prediction accuracy across different risk categories. False positive rates require ongoing measurement to prevent alert fatigue. Detection coverage metrics ensure models identify diverse money laundering typologies effectively [10].

Model governance processes document complete development lineage. Training data provenance records data sources, collection methodologies, and quality assurance procedures. Feature engineering decisions receive detailed documentation explaining variable construction and transformation logic. Hyperparameter selections undergo systematic evaluation comparing multiple configuration alternatives. Version control systems maintain audit trails of model modifications across development iterations. Regulatory examination requires demonstration of sound model development practices following established industry standards [10].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Five-layer governance frameworks structure AI oversight responsibilities across organizational levels. Strategic governance establishes institutional policies regarding acceptable AI applications and risk tolerances. Tactical governance translates high-level policies into specific implementation requirements and controls. Operational governance manages day-to-day model monitoring and performance tracking. Technical governance ensures suitable architectural selections and engineering practices. Ethical governance addresses fairness, duty, and societal effect concerns. Each layer maintains clear accountability structures defining roles and responsibilities for governance activities [10].

Continuous monitoring detects model degradation and concept drift over time. Statistical distributions of input features may shift as customer populations evolve. Relationship patterns between features and target variables can change as money laundering techniques adapt. Performance metrics tracked across rolling time windows identify emerging problems requiring model retraining or architectural modifications. Automated alerting systems notify governance teams when performance falls below acceptable thresholds, triggering formal review processes [10].

Framework Element	Implementation Method	Regulatory Benefit
Feature Attribution	SHAP values, LIME techniques	Individual contribution quantification
Visual Explanation	Attention mechanisms	Decision factor highlighting
Model Documentation	Training data provenance	Complete development lineage
Performance Monitoring	Accuracy tracking across segments	Fairness validation
Strategic Governance	Institutional policy establishment	Risk tolerance definition
Technical Governance	Architecture validation	Engineering practice compliance

Table 4. Explainability and Governance Framework Components [9, 10].

Conclusion

Ai-pushed automation essentially transforms compliance operations from reactive duties into proactive intelligence talents. Traditional rule-based structures struggle with record variability, behavioral complexity, and adaptive crook strategies. Machine learning models process high-dimensional transaction features, identifying patterns invisible to conventional threshold-based monitoring. Graph neural networks reveal hidden entity relationships across complex ownership structures and transaction networks. Behavioral analytics establish dynamic baseline profiles, detecting subtle deviations indicating potential account takeover or structuring activities. Computer vision and natural language processing enable automated identity verification across diverse document formats and languages.

Explainability mechanisms address regulatory transparency requirements through attention mapping, SHAP value decomposition, and local interpretable model approximations. Compliance officers receive clear explanations highlighting which transaction attributes or document features influenced specific risk classifications. Human-in-the-loop architectures permit expert feedback on automated anomaly detection, where an anomaly is any behavior pattern that strays from the normal behavior pattern. Some anomalies do not require investigation. Governance frameworks assign oversight capacities to institutional levels. Model validation processes ensure fair treatment across demographic segments. Continuous monitoring detects performance degradation and concept drift requiring

intervention. Training data provenance, feature engineering documentation, and hyperparameter selection rationale maintain complete audit trails for regulatory examination.

Financial institutions using AI-enabled compliance systems will be well-positioned now and into the future. To implement it, one must work with compliance specialists, data scientists, and technology architects. Success requires consideration of the balance between automation efficiency and accountability. The challenge involves establishing appropriate governance structures, validation methodologies, and transparency mechanisms satisfying operational and regulatory requirements. AI represents operational necessity rather than competitive advantage as threat actors develop increasingly sophisticated evasion techniques. Enhanced detection capabilities, reduced false positive rates, and accelerated processing times demonstrate tangible benefits justifying technology investments. The evolution toward intelligent automation continues to reshape financial crime prevention.

References

[1] Samuel Aidoo, "The Cost of AML Compliance," 2025. [Online]. Available: https://www.researchgate.net/profile/Samuel-Aidoo-2/publication/393655422_The_Cost_of_AML_Compliance/links/687451e9ae516743559cb8e7/The-Cost-of-AML-Compliance.pdf

[2] MOHANNAD ALKHALIL et al., "Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering," IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9328094

[3] UTKU GÖRKEM KETENC et al., "A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering," IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9399421

[4] Joana Lorenz et al., "Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity," ACM, 2020. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3383455.3422549

[5] Yi Sun et al., "Deep Learning Face Representation by Joint Identification-Verification," NeurIPS. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/2014/file/2f9d64528ced0ea456b16aa7268f3463-Paper.pdf

[6] STEFANO FERRETTI et al., "Enhancing Anti-Money Laundering Frameworks: An Application of Graph Neural Networks in Cryptocurrency Transaction Classification," IEEE Access, 2025. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10930500

[7] Oyewale Oyedokun et al., "A Comprehensive Review of Machine Learning Applications in AML Transaction Monitoring," International Journal Of Engineering Research And Development, 2024. [Online]. Available: https://www.researchgate.net/profile/Oyewale-Oyedokun/publication/388277251

[8] Xueying Ding et al., "From Detection to Action: a Human-in-the-loop Toolkit for Anomaly Reasoning and Management," ACM, 2023. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3604237.3626872

[9] DATTATRAY VISHNU KUTE et al., "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review," IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9446887

[10] Avinash Agarwal and Manisha J. Nene, "A Five-Layer Framework for AI Governance: Integrating," arXiv, 2025. [Online]. Available: https://arxiv.org/pdf/2509.11332