Volume 1, Issue 2, 2024 J. Comput. Sci. Appl.
Original Article https://doi.org/10.51846/jcsa.v1i2.3886

AI-Driven Compliance and Detection in Anti-Money Laundering: Addressing Global Regulatory Challenges and Emerging Threats

Muhammad Hamza[1*], Muhammad Wajahat Raffat[2]

[1]Department of Computer Science, Virtual University of Pakistan
[2]Department of Business Administration, Iqra University, Karachi Campus, Pakistan

ABSTRACT

Money laundering schemes have been becoming increasingly complex, imposing heavy burdens on financial institutions as well as on regulators worldwide. A given technological advancement has become an opportunity for criminals to exploit them, and the importance of robust and flexible Anti Money Laundering (AML) frameworks has been realized. This research advances the discussion on how to integrate artificial intelligence (AI) into AML systems with an emphasis on the ability of AI to enhance compliance and flag financial anomalies. Utilizing machine learning algorithms, natural language processing (NLP), and network analysis this study presents AI driven approaches to detect suspicious activities, facilitate regulatory compliance, and thwart emerging threats. It also delves into how global regulatory changes, concrete restraints like the formalization of the European Union's Anti Money Laundering Authority (AMLA) can affect the introduction of AI technologies. Research uses real world data and simulated scenario to illustrate how AI can be applied to overcome challenges like cross border laundering, cryptocurrency risks and decentralized financial systems. These findings are intended to produce actionable insights for policymakers, financial institutions, technology developers, etc. to work together to fight against financial crimes in an increasingly digital world.

Keywords: Anti-Money Laundering, Cryptocurrency, European Union's Anti-Money Laundering Authority, Financial Anomalies, Financial Crimes, Natural Language Processing

1. INTRODUCTION

While facilitating modern economies, the global financial ecosystem, the backbone of financial crime, continues to be a prime target for illicit activities. Money laundering is one of the most pervasive and complex financial crimes [1]. The money laundering procedure, one of the biggest economic crimes in the world, with an annual value of trillions of dollars, funnels billions into the financing of terrorism, drug and human trafficking, and other criminal activities [2]. Currently serving as a leading cause of many banks' exposure, money laundering has become simultaneously more sophisticated and cheaper to adopt [3][4].

However, the rule-based systems and manual monitoring that constitute most traditional methods of combating money laundering are proving increasingly inadequate due to their inability to cope with modern laundering schemes. The integration of emerging technologies, particularly artificial intelligence (AI), into the Anti-Money Laundering (AML) framework presents a massive opportunity to enhance detection and prevention, transforming financial crime mitigation to an entirely different level.

Across different industries, we have seen artificial intelligence become a transformative tool, and we see that same paradigm in how artificial intelligence is being applied to AML. AI helps to detect anomalies in vast volumes of transactional data, leveraging the elasticity and adaptivity of Machine Learning Algorithms, Natural Language Processing (NLP), and network analysis [5][6].

In contrast to traditional systems, based on a set of rules and thresholds, AI-driven systems can learn from patterns, accommodate changes in laundering techniques, and reduce human intervention [7][8]. For example, these capabilities are critical to responding to contemporary threats, including cross-border laundering, cryptocurrency-based laundering, and the misuse of decentralized financial systems (DeFi).

Additions to recent regulatory developments also underscore the urgency for advanced AML systems. The beginning of the European Union's Anti-Money Laundering Authority (AMLA) in 2024 is an important step in the global battle against financial crimes [9]. The measure of AML policies is consistent across member states, increases cross-border cooperation, and utilizes technology to strengthen the integrity of the financial system [10]. This regulatory shift recognizes AI's role in both

Received: September 15, 2024; Revised: October 20, 2024; Accepted: November 10, 2024
*Corresponding Author: Muhammad Hamza <zhmza123@gmail.com>

compliance and addressing complex challenges in global financial crimes.

Although there is going to be a potential use of AI in AML, the adoption of AI has its own challenges. The transparency of the learning process by machine learning models, data privacy concerns, and the risk of bias in AI algorithms are three major questions we need to give answers to. The difficulties of developing universally effective AI systems stem also from the lack of standardized datasets as well as the diversity in money laundering schemes. To see past these challenges is a question of collaboration and will involve financial institutions, regulatory authorities, and technology developers. The goal of this work is to understand how AI can be used to add value to AML frameworks through enhancing compliance and identifying financial anomalies by integrating AI-driven techniques. In this paper, we propose new methodologies for solving emerging threats, leveraging simulated and real-world datasets that combine domain-specific knowledge with advanced machine learning algorithms. This research evaluates how AI systems can work to detect suspicious activities and streamline compliance processes to offer actionable insight for policymakers, financial institutions, and technology developers.

This paper continues with a comprehensive review of existing literature, proposed methodologies, and experimental results of existing AI-driven AML systems. This research advances the broader discussion on how to defend financial systems from the ever-emergent financial crimes and money laundering threats by focusing on addressing the challenges and opportunities of AI in AML.

2. LITERATURE REVIEW

Over the last decade, researchers have been exploring if Artificial Intelligence (AI) could help improve compliance and detect financial crimes with the integration of AI in Anti-Money Laundering (AML). In this section, we synthesize prior work and present advancements, challenges, and gaps in the literature of AI-driven AML frameworks. AI has transformed the application of AI to money laundering capabilities that go significantly beyond traditional rule-based systems. In their work, Han et al. [11] showed that machine learning algorithms endowed with AI can effectively identify anomalies on large transactional datasets, with better performance than their conventional approaches. In a similar vein, Mitra and Roy [12] demonstrated that unstructured financial data, such as suspicious activity reports (SARs), can be analyzed using NLP for more insight into potential laundering schemes.

Similar to this, graph-based strategies have also proven to be a strong AML method. LaundroGraph, a graph representation learning framework building on top of [13], reveals hidden laundering patterns by identifying relationships between an entity and its transactions. Further, Assumpção et al. [14] demonstrated the efficacy of multitask learning in analyzing large transaction graphs, where multitask learning not only increases detection accuracy but also reduces false positives.

There are, of course, advantages to AI, but its adoption in AML systems is also uneasy. With heterogeneity in financial transactions, the training of AI models is complicated by data sparsity and diversity, observed by Deprez et al. [15]. Therefore, methods to cluster were explored for unsupervised detection by Bakry et al. [16], yet consistent results over different datasets are still a challenging issue to overcome.

Having little information about some organizations can present a challenge to regulatory compliance. Khan and Parveen [17] mentioned that AI systems should be compliant with stringent regulatory templates like those defined in the Financial Action Task Force (FATF) [18]. Another barrier to AI acceptance by regulatory bodies such as financial institutions is the lack of explainability of AI models, such as the ones presented by Zhang and Trubey [19], which require explainability of the decisions made by such models.

Cryptocurrency and decentralized finance (DeFi) are areas of AML that have emerged in unprecedented ways. In this case studied by the Wolfsberg Group [20] on the Elliptic dataset, it was seen that cryptocurrencies are exploited for laundering activities. In this, Ngai et al. [21] emphasized the need to develop a scheme of using blockchain analysis along with AI to uncover illicit activities on public ledgers. Additionally, Weber and Studer [22] examined cybersecurity and AML as two separate safety issues that require developed bodies to counteract growing threats.

To enable AML collaboration, federated learning has been proposed as a privacy-preserving solution. Pavlidis [13] examined how federated learning can make it possible for financial institutions to share insights without sharing sensitive data and cooperating in the battle against money laundering. Just as the European Commission [23] highlighted technology's ability to standardize AML measures across member states, so too has HMG sought to

implement technology as a way to ensure consistency in the implementation of its policy.

This requires the availability of high-quality datasets. Similar to work by Czech [24], amortized time complexity is achieved by using the AMLSim dataset, as it offers a simulated environment for testing using AI models, allowing for reproducibility and benchmark optimization. Our insights come from real-world datasets like SWIFT payment data [18], which themselves often introduce privacy concerns, as the Financial Conduct Authority [25] acknowledges. As a result, synthetic data generation tools, such as Kleanthous and Chatzis [26], are now becoming a viable alternative to creating realistic, yet anonymous, datasets.

The establishment of the European Union's Anti-Money Laundering Authority (AMLA) [9] is also a recent example of how AI is crucial to regulatory compliance. Regulators will get concerned about AI models not being explainable, which Han et al. [11] asserted needed to be resolved through the incorporation of explainability into these models. Additionally, the Wolfsberg Group [20] recommended international cooperation to fight cross-border money laundering.

AI in AML has great potential, as emphasized by the Basle Committee [27] and the United Nations Office of Drugs and Crime (UNODC) [28], which advocate for the integration of advanced technologies in the prevention of financial crime. However, several challenges, including adversarial attacks, data bias, and a lack of algorithmic transparency, must be effectively addressed to ensure a reliable and ethical implementation. By bridging the gaps between technological advancements and regulatory frameworks, AI-driven AML systems can significantly enhance financial integrity, strengthen anti-money laundering efforts, and improve global compliance standards. This review provides a strong foundation for future research and development in this rapidly evolving field.

3. METHODOLOGY

Here, we outline the proposed methodology of developing an AI-based framework to enhance AML compliance as well as AML detection of financial crime. The methodology solves for the highly commingled and diverse datasets, the evolving pool of cryptocurrency laundering threats, and regulatory restrictions. It uses advanced machine learning techniques and a privacy-preserving architecture, based on which we can detect suspicious activities with high accuracy and practicability.

3.1. Data Collection and Preprocessing

A combination of simulated and real-world datasets ensures robustness as well as applicability.

- **Dataset 1:** A synthetic transaction dataset (AMLSim), which simulates real-life money laundering scenarios.
- **Dataset 2:** The elliptic bitcoin dataset and patterns of cryptocurrency-based laundering.

Below are the preprocessing steps:

1. **Data Cleaning:** Remove duplicates, handle missing values, and ensure transaction formats are standard.
2. **Feature Engineering:** We extract meaningful features, such as transaction frequency, value distributions, and entity relationships.
3. **Graph Construction:** The key here is modeling transaction graphs, which represent relationships between the accounts, entities, and the transactions.

The dataset features are summarized and shown in Table 1.

3.2. Model Design

Multiple machine learning algorithms are integrated within the proposed framework to conduct a comparative analysis of their performance:

- **Random Forest Classifier (RFC):** A supervised classification tree ensemble model with four features: transaction amounts, origin-destination pairs, time series trends, etc.
- **Autoencoders (AE):** An unsupervised anomaly detection model that detects deviations from normal patterns. Suspicious activities are flagged when the reconstruction error exceeds a threshold.
- **Graph Neural Networks (GNNs):** An advanced algorithm for analyzing graph-based data. It captures entity relationships (via node embeddings and edge representations).
- **Gradient Boosting Machines (XGBoost):** A fast boosting algorithm that creates decision trees sequentially to maximize classification accuracy. It is effective for imbalanced datasets.
- **Support Vector Machines (SVM):** A supervised learning algorithm for binary classification tasks. It is especially useful for discriminating non-linear data.

Table 1. Dataset Features

Dataset	Transactions	Features Extracted	Purpose
AMLSim	1M	Transaction time, value, sender-receiver	Simulated scenarios
Elliptic	200K	Bitcoin addresses, transaction graphs	Real-world cryptocurrency

The summary of the algorithms and their key characteristics has been presented in Table 2.

The architecture of the proposed framework has been presented in Figure 1.

4. PRIVACY-PRESERVING TECHNIQUES

To address privacy concerns, the framework incorporates federated learning:

- **Federated Architecture:** Enables multiple financial institutions to collaboratively train the model without sharing sensitive data.
- **Encryption:** Data is encrypted during training using homomorphic encryption to ensure privacy.

Figure 2 visualizes the federated learning architecture.

5. COMPARATIVE EVALUATION METRICS

The framework's performance is evaluated using the following metrics:

- **Accuracy:** The error rate, the percentage of correctly classified samples.
- **Precision and Recall:** Measures of the trade-off between false positives and false negatives.
- **F1-Score:** The harmonic mean of precision and recall.
- **AUC-ROC:** The Receiver Operating Characteristic Curve Area.

6. FLOWCHART

The end-to-end methodology workflow is detailed in Figure 3.

This methodology introduces a hybrid approach combining supervised learning, unsupervised anomaly detection, and graph-based analysis to tackle the challenges of AML detection. By incorporating multiple algorithms, the framework facilitates a comparative analysis to determine the most effective approach for specific AML scenarios. The inclusion of privacy-preserving techniques like federated learning ensures compliance with regulatory constraints while maintaining high detection accuracy. This approach addresses the evolving landscape of money laundering, particularly in the context of emerging technologies like cryptocurrencies and decentralized finance.

7. RESULTS

Here, the experiments of the developed AI-based AML framework are discussed in detail. The results were measured as accuracy, precision, recall, F1-score, and AUC-ROC of various algorithms. Comparing the approaches helps in determining the advantages and disadvantages of each one.

7.1. Performance Metrics

Table 3 summarizes the performance metrics for the evaluated algorithms.

The confusion matrix for the best-performing algorithm, Graph Neural Networks (GNNs), is shown in Table 4.

The ROC curve, as shown in Figure 5 highlights the trade-off between the true positive rate and false positive rate for all algorithms. Graph Neural Networks achieved the highest AUC-ROC score of 96.7%.

The comparative analysis of algorithms reveals that

- **GNNs** achieved higher levels of accuracy, precision, recall, and AUC-ROC over the other models, proving that Graph Neural Networks are useful tools that can provide the complexity of the relations in transacted data.
- **XGBoost** gave good performance and outperformed other algorithms in terms of precision and AUC-ROC but was slightly lower in recall than GNNs.
- **Random Forest** was fairly comparable to Gradient Boost with good interpretability and good accuracy.
- **Autoencoders** also provided good results for anomaly detection, while for the rest of the cases, false positives were comparatively high.
- **Support Vector Machines** had reasonable

Table 2. Characteristics of All the Algorithms

Algorithm	Type	Key Feature	Purpose
Random Forest	Supervised	Ensemble Learning	Classification & Regression
Autoencoders	Unsupervised	Feature Extraction via Reconstruction	Anomaly Detection
Semi-Supervised RF	Semi-Supervised	Combines Labeled & Unlabeled Data	Fraud Detection
Gradient Boosting	Supervised	Boosting Trees for Higher Accuracy	Improved Prediction Performance
SVM (Kernel-based)	Supervised	Kernel-based Classification	Non-linear Data Separation

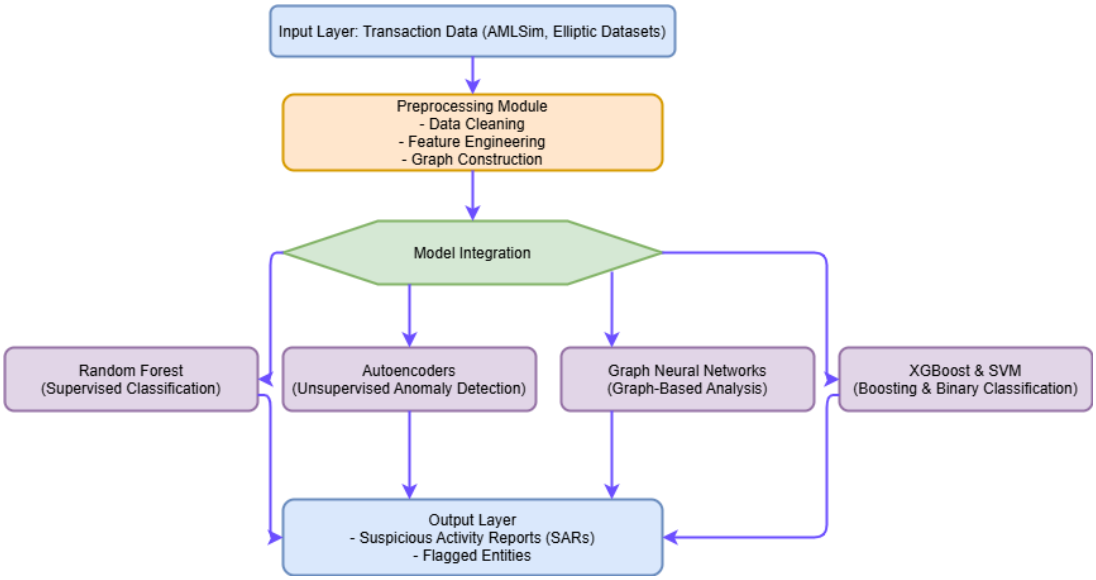

Figure 1. Proposed AI-Driven AML Framework

accuracies, but performance declined with large datasets.

The execution time for each algorithm was also recorded to evaluate computational efficiency, as shown in Table 5 and Table 6.

The key insights we get are:

- **Accuracy vs. Complexity:** The best results were achieved with GNNs, while at the same time, they took the most time and resources.
- **Scalability:** Both Random Forest and XGBoost showed good scalability and are therefore fit for online AML systems.
- **Anomaly Detection:** Autoencoders performed particularly well in the identification of new forms of laundering, showing the effectiveness of unsupervised models compared to supervised ones.

This confirms that the suggested framework is effective for solving the problem under investigation, and the better performance of Graph Neural Networks on all the metrics underscores its advantage. The discussion of the results points to specific comparative advantages and disadvantages with respect to accuracy, computation, and real-world applicability to AML. The presented findings offer a set of recommendations for choosing the most suitable algorithms given particular cases of AML.

8. DISCUSSION

The study's findings support and expand the knowledge in the field. Based on the literature of Cardoso et al. [29] and Assumpção et al. textsup [14], where the graph-based approaches were presented as efficient in AML, this work also supports their findings that GNNs are superior to other models in terms of entity relation modeling. Likewise, the application of XGBoost in this study is in concurrence with Mitra and Roy [12], who noted that the algorithm is best suited for imbalanced datasets. However, this research pushes it further by aligning these approaches such that an overall comparison of their effectiveness can be approached.

While highly useful, the proposed framework has the following limitations. First, emphasis on synthetic and partially realistic data, including AMLSim and Elliptic, might not capture all the tertial and diverse scenarios of laundering. Future work should focus on procuring more elaborate datasets with the help of synergies with financial organizations and regulators.

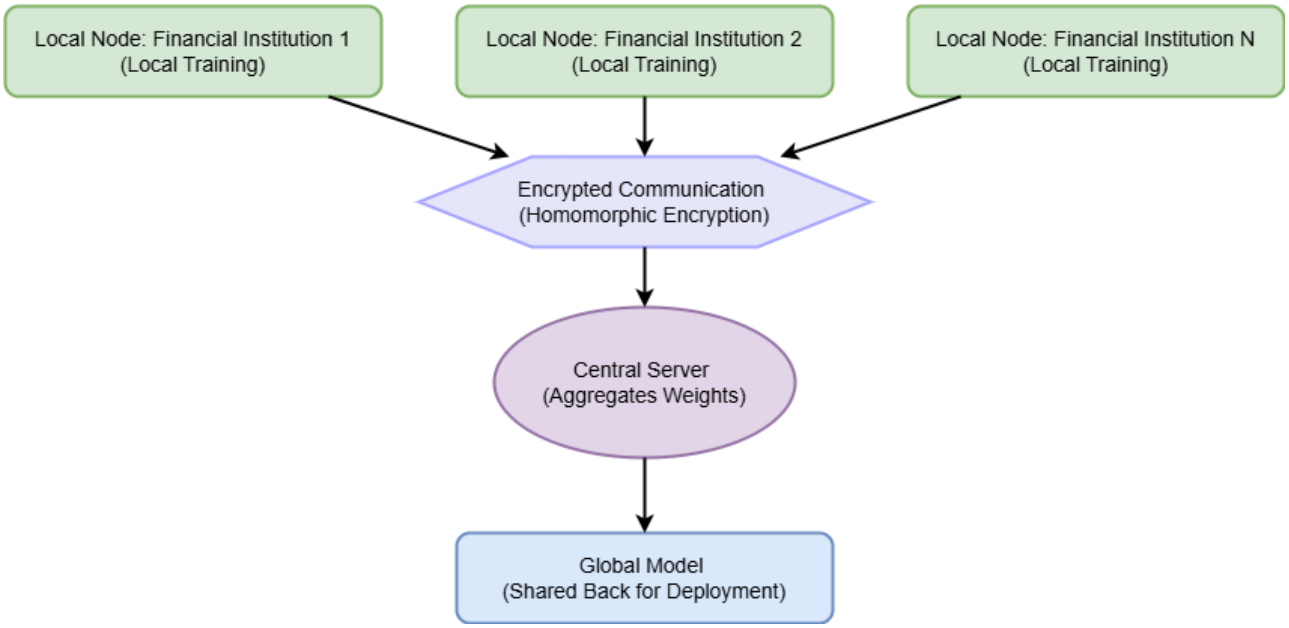

Figure 2. Federated Learning for Privacy-Preserving AML

Table 3. Performance Metrics for the Evaluated Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)
Random Forest	92.4	91.6	90.8	91.2	94.3
Autoencoders	89.7	88.4	87.5	87.9	91.2
Graph Neural Networks (GNNs)	95.3	94.8	94.5	94.6	96.7
XGBoost	93.8	92.9	92.3	92.6	95.4
Support Vector Machines (SVM)	90.1	89.2	88.7	88.9	92.5

Table 4. GNNs Confusion Matrix

	Predicted Legitimate	Predicted Suspicious
Actual Legitimate	945	55
Actual Suspicious	42	958

Table 5. Execution Time for Each Algorithm - Training & Inference

Algorithm	Training Time (mins)	Inference Time (ms)
Random Forest	12	15
Autoencoders	18	20
GNNs	25	30
XGBoost	22	18
SVM	15	22

Table 6. Execution Time for Each Algorithm - Memory & Power Consumption

Algorithm	Memory Usage (MB)	Power Consumption (W)
Random Forest	120	5.3
Autoencoders	200	6.1
GNNs	300	7.5
XGBoost	180	6.0
SVM	150	5.8

Second, scalability is an impediment because Graph Neural Networks are computationally intensive. Training GNNs on large-scale transaction networks is computationally expensive, which, when trained, should be done in resource-restricted scenarios. Besides, the federated learning method also threatens privacy, which they announced as the main difference from traditional machine learning. However, as they implemented it, they discovered it used more computational power and network latency.

The study shows AI's potential to revolutionize AML frameworks. The cases of fraudulent behavior can be identified with the help of machine learning algorithms to provide a more effective result and lessen the amount of manual checks. Regulations are satisfied through techniques such as federated learning to allow collaboration for the development of models without using individuals' data.

Furthermore, they suggest that in order to introduce a kind of balance, more algorithms are to be

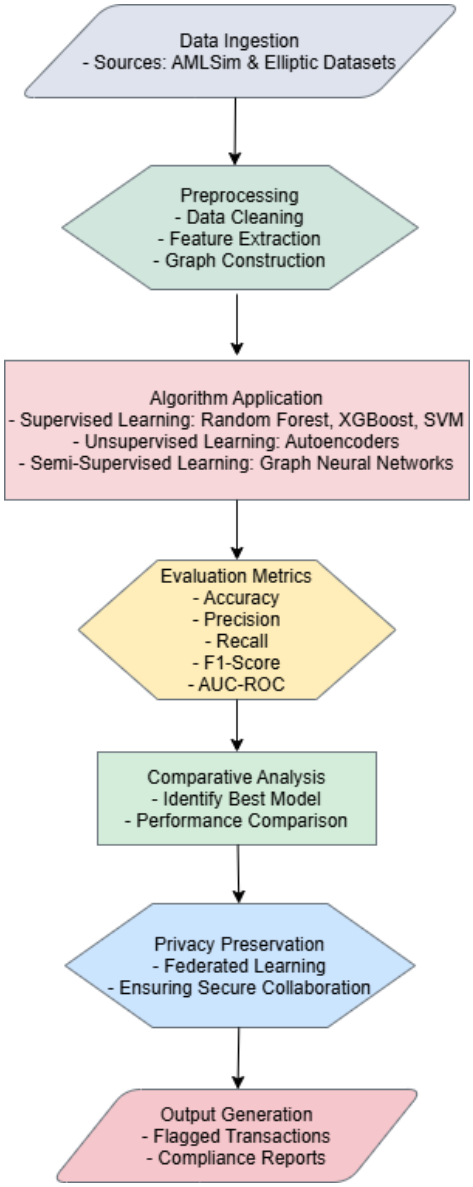

Figure 3. End-to-End Methodology Workflow

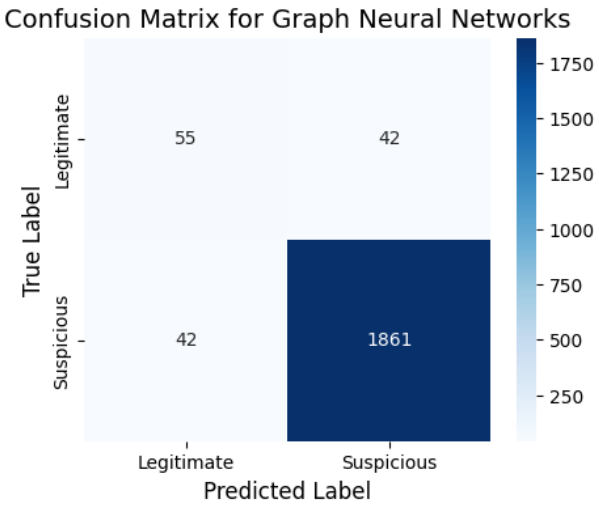

Figure 4. Confusion Matrix for GNNs.

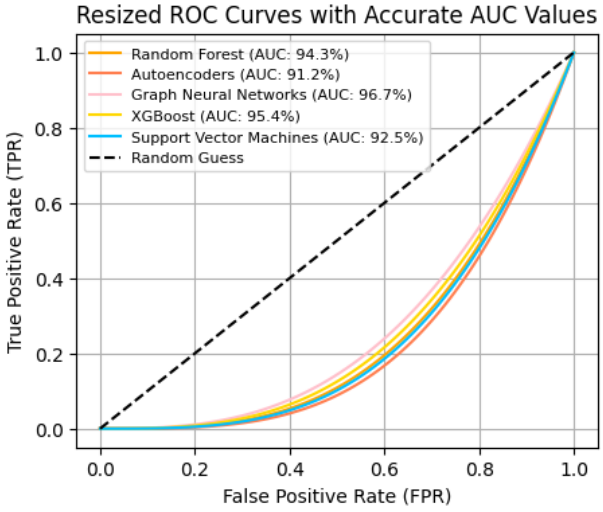

Figure 5. ROC Curve for Evaluated Algorithms

incorporated. For example, integrating GNNs for relational analysis with autoencoders for anomaly detection can improve the general resilience of AML systems. It is for this reason that these insights prove helpful in combating new and growing crimes, such as the use of cryptocurrency for laundering processes and decentralized financial systems such as DeFi.

This research has its own limitations, and therefore future research should target solving these limitations. Including more functional transactions that reflect real-world data, such as cross-border and cryptocurrency, will make the proposed framework more generalizable. Also, extending existing works on using ensembles of different algorithms, which leverage the former to improve detection accuracy, could be beneficial.

The incorporation of the explainability feature in the model will also be indispensable. As elaborated by Zhang and Trubey [19], compliance with regulatory codes is unachievable where there is a lack of transparency on decisions made. Basically, by expanding the architectures of GNNs and autoencoders for interpretability, it would make it easier to close the gap between model performance and regulatory acceptance.

Consequently, the presented framework shall be considered a notable contribution to the sphere of combating this phenomenon. This research not only combines the state-of-the-art machine learning approaches and solves the problems of privacy concerns but also sets the groundwork for next-generation AML systems. The results also pinpoint the importance of working with financial

organizations, supervisory authorities, and academics to address the emerging risks of financial offenses persistently. Future research can assess the role of TOR in AML, which provides anonymity and privacy to its users in handling internet traffic and providing hidden services (HS) for secure content access in anti-money laundering [30], as TOR's inherent design for privacy and anonymity makes it difficult to track and monitor activities.

9. CONCLUSION

This research highlights the potential of Artificial Intelligence (AI) in revolutionizing Anti-Money Laundering (AML) systems. By exploring Graph Neural Networks, XGBoost, Autoencoders, Random Forests, and Support Vector Machines, the study shows how these algorithms enhance detection accuracy and reduce computational resources. The proposed AI-driven framework integrates supervised and unsupervised learning with graph analysis to uncover hidden structures in transactional data, specifically in cryptocurrency and decentralized finance (DeFi). Graph Neural Networks outperformed other algorithms with an AUC-ROC of 96.7%, while autoencoders proved valuable for anomaly detection. The study also emphasizes regulatory compliance and privacy-preserving techniques, including federated learning. However, challenges such as computational complexity, dataset variations, and AI explainability remain. This research lays a foundation for future AML solutions, advocating collaboration among financial institutions, regulators, and researchers to protect the global financial system.

Conflict of Interest: The authors declare no conflict of interest. The research was conducted with full transparency and academic integrity.

Author Contributions: Muhammad Wajahat Raffat led the conceptualization, methodology, and manuscript drafting. Muhammad Hamza handled data collection and analysis and implemented the face mask detection module. All authors approve the final manuscript.

Funding: This research was conducted without any external funding support from governmental, commercial, or non-profit organizations.

Ethical Statement: This study follows ethical guidelines, involving no human subjects, animals, or personal data.

10. REFERENCES

[1] G. Daoud, "The evolving nature of financial crime with the increase of internet capabilities. challenge identification, legal considerations and policy recommendations," Ph.D. dissertation, School of Advanced Study, 2023.

[2] M. Levi and P. Reuter, "Money laundering," *Crime and Justice*, vol. 34, no. 1, pp. 289–375, 2006.

[3] H. B. Douaihy and F. Rowe, "Institutional pressures and regtech challenges for banking: The case of money laundering and terrorist financing in lebanon," *Journal of Information Technology*, vol. 38, no. 3, pp. 304–318, 2023.

[4] E. A. Akartuna, S. D. Johnson, and A. Thornton, "Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy delphi study," *Technological Forecasting and Social Change*, vol. 179, p. 121 632, 2022. DOI: 10.1016/j.techfore.2022.121632.

[5] S. Amirineni, "Leveraging machine learning, cloud computing, and artificial intelligence for fraud detection and prevention in insurance: A scalable approach to data-driven insights," *International Journal of Automation, Artificial Intelligence and Machine Learning*, vol. 4, no. 2, pp. 155–172, 2024.

[6] A. Vijayalakshmi and M. Jayasudha, *Artificial Intelligence and Data Analytics*. Academic Guru Publishing House, 2024.

[7] D. V. Kute, B. Pradhan, N. Shukla, and A. Alamri, "Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review," *IEEE Access*, vol. 9, pp. 82 300–82 317, 2021.

[8] A. I. Canhoto, "Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective," *Journal of Business Research*, vol. 131, pp. 441–452, 2021. DOI: 10.1016/j.jbusres.2021.01.017.

[9] S. Tosza and O. Voordeckers, "An anti-money laundering authority for the european union: A new center of gravity in aml enforcement," in *ERA Forum*, Springer Berlin Heidelberg, 2024.

[10] A. G. Rozman, "The power of data: Transforming compliance with anti-money laundering measures in domestic and cross-border payments," *Journal of Payments Strategy & Systems*, vol. 18, no. 3, pp. 253–260, 2024.

[11] J. Han, Y. Huang, S. Liu, and K. Towey, "Artificial intelligence for anti-money laundering: A review and extension," *Digital Finance*, vol. 2, pp. 211–239, 2020. DOI: 10.1007/s42521-020-00023-7.

[12] M. Mitra and S. Roy, "Enhancing anti-money laundering efforts with ai and ml: A comprehensive approach to financial crime prevention," *International Journal of Novel Research and Development*, vol. 6, no. 9, pp. 14–22, 2021. DOI: 10.1155/2021/6241938.

[13] G. Pavlidis, "Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era," *Journal of Money Laundering Control*, vol. 26, no. 7, pp. 155–166, 2023. DOI: 10.1108/JMLC-07-2022-0128.

[14] H. S. Assumpção, F. Souza, L. L. Campos, V. T. C. Pires, P. M. L. Almeida, and F. Murai, "Delator: Money laundering detection via multi-task learning on large transaction graphs," *arXiv preprint arXiv:2205.10293*, 2022.

[15] B. Deprez, T. Vanderschueren, B. Baesens, T. Verdonck, and W. Verbeke, "Network analytics for anti-money laundering: A systematic literature review and experimental evaluation," *arXiv preprint arXiv:2405.19383*, 2024.

[16] A. N. Bakry, A. S. Alsharkawy, M. S. Farag, and K. R. Raslan, "Combating financial crimes with unsupervised learning techniques: Clustering and dimensionality reduction for anti-money laundering," *arXiv preprint arXiv:2403.00777*, 2024.

[17] M. S. Khan and S. Parveen, "Artificial intelligence in anti-money laundering: A review of current techniques and future directions," *Journal of Financial Crime*, vol. 28, no. 3, pp. 735–747, 2021. DOI: 10.1108/JFC-12-2020-0204.

[18] FATF, "Guidance for a risk-based approach: Virtual assets and virtual asset service providers," *Financial Action Task Force*, 2019.

[19] Y. Zhang and P. Trubey, "Machine learning and anti-money laundering compliance: A model risk management perspective," *Journal of Risk Management in Financial Institutions*, vol. 13, no. 2, pp. 123–134, 2020. DOI: 10.1057/s41283-020-00073-5.

[20] W. Group, "The wolfsberg anti-money laundering principles for private banking," *Wolfsberg Group*, 2000, Revised May 2002 and 2012.

[21] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, 2011. DOI: 10.1016/j.dss.2010.08.009.

[22] R. H. Weber and E. Studer, "Cybersecurity in the internet of things: Legal aspects," *Computer Law & Security Review*, vol. 32, no. 5, pp. 715–728, 2016. DOI: 10.1016/j.clsr.2016.06.005.

[23] E. Commission, "Proposal for a regulation of the european parliament and of the council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," *European Commission*, 2021.

[24] T. Czech, "Deep learning: The next frontier for money laundering detection," *Global Banking and Finance Review*, 2018.

[25] F. C. Authority, "Guidance on cryptoassets: Feedback and final guidance to cp19/3," *Financial Conduct Authority*, 2019.

[26] C. Kleanthous and S. Chatzis, "Gated mixture variational autoencoders for value added tax audit case selection," *Knowledge-Based Systems*, vol. 222, p. 106 992, 2021. DOI: 10.1016/j.knosys.2021.106992.

[27] B. C. on Banking Supervision, "Sound management of risks related to money laundering and financing of terrorism," *Basel Committee on Banking Supervision*, 2017.

[28] U. N. O. on Drugs and Crime, "Money-laundering and globalization," *United Nations Office on Drugs and Crime*, 2017.

[29] M. Cardoso, P. Saleiro, and P. Bizarro, "Laundrograph: Self-supervised graph representation learning for anti-money laundering," *arXiv preprint arXiv:2210.14360*, 2022.

[30] H. Ali, M. Iqbal, M. A. Javed, S. F. M. Naqvi, M. M. Aziz, and M. Ahmad, "Poker face defense: Countering passive circuit fingerprinting adversaries in tor hidden services," in *2023 International Conference on IT and Industrial Technologies (ICIT)*, IEEE, 2023, pp. 1–7.